Astaro Security Gateway

バージョン8.200

管理ガイド

日付：2011/11/21 16:56 UTC

当文書に記載されている仕様と情報は、予告なく変更される場合があります。例で使用されている会社、名前、データは、明記されている場合を除き架空のものです。Astaro GmbH & Co. KGの書面による明示的な許可なく、当文書の一部または全体を手段を問わず複製または配布することは、いかなる理由においても許可されません。本マニュアル原文の翻訳には、「マニュアル原文の翻訳(Translation of the original manual)」と記載しなければなりません。

© 2000–2011 Astaro GmbH & Co. KG.
All rights reserved.
Amalienbadstraße 41/Bau 52,
76227 Karlsruhe,
Germany
http://www.astaro.com

Astaro Security Gateway&、Astaro Mail Gateway、Astaro Web Gateway、Astaro Command Center、Astaro Gateway Manager、およびWebAdminはAstaro GmbH & Co. KGの商標です。CiscoはCisco Systems Inc.の登録商標です。iOS はApple Inc.の商標です。LinuxはLinus Torvalds氏の商標です。他のすべての商標は、該当する所有者の財産です。

限定保証

当文書に記載されている情報の正確性は保証されません。コメントや修正については、documentation@astaro.comまでご連絡ください。

目次

1インストール 13
1.1参考資料 13
1.2システム要件 13
1.2.1UPSデバイスのサポート 15
1.2.2RAIDサポート 16
1.3インストール手順 16
1.3.1インストール中の主な機能 16
1.3.2インストール中の特別なオプション 17
1.3.3インストール中 Astaro Security Gateway 17
1.4基本設定 20
1.5バックアップリストア 26

2WebAdmin 29
2.1WebAdminメニュー 30
2.2ボタンバー 31
2.3リスト 32
2.4ダイアログボックス 33
2.5ボタンとアイコン 33
2.6オブジェクトリスト 35

3ダッシュボード 37
3.1フローモニタ 40

4マネジメント 43
4.1システム設定 43
4.1.1組織 44
4.1.2ホスト名 44
4.1.3日付と時刻 44
4.1.4シェルアクセス 48
4.1.5設定またはパスワードのリセット 49
4.2WebAdmin設定 50
4.2.1一般 50
4.2.2アクセスコントロール 51
4.2.3セキュリティ 52
4.2.4HTTPS証明書 53
4.2.5ユーザ設定 54
4.2.6詳細 56
4.3ライセンス 57
4.3.1ライセンスの取得方法 57

4.3.2オンデマンドライセンス 58
4.3.3クラシックライセンス 61
4.3.4概要 63
4.3.5インストール 64
4.3.6アクティブなIPアドレス 65
4.4Up2Date 66
4.4.1概要 66
4.4.2設定 69
4.4.3詳細 70
4.5バックアップ/リストア 71
4.5.1バックアップ/リストア 71
4.5.2自動バックアップ 74
4.6ユーザポータル 75
4.6.1グローバル 77
4.6.2詳細 79
4.7通知 80
4.7.1グローバル 80
4.7.2通知 81
4.7.3詳細 81
4.8カスタマイズ 82
4.8.1グローバル 82
4.8.2Webフィルタ 83
4.8.3ダウンロードマネージャ 84
4.8.4SMTP/POP3プロキシ 86
4.9SNMP 87
4.9.1クエリ 87
4.9.2トラップ 90
4.10集中管理 91
4.10.1Astaro Command Center 91
4.11冗長化(HA) 94
4.11.1ハードウェアとソフトウェアの要件 95
4.11.2ステータス 96
4.11.3システムステータス 98
4.11.4設定 98
4.12シャットダウンとリスタート 103

5定義およびユーザ 105

5.1ネットワーク定義 105
5.2サービス定義 109
5.3期間定義 112
5.4ユーザ&グループ 113

5.4.1ユーザ 113
5.4.2グループ 116
5.5クライアント認証 119
5.6認証サーバ 120
5.6.1グローバル設定 121
5.6.2サーバ 122
5.6.2.1eDirectory 122
5.6.2.2Active Directory 124
5.6.2.3LDAP 128
5.6.2.4RADIUS 130
5.6.2.5TACACS+ 133
5.6.3シングルサインオン(Single Sign-On) 134
5.6.4詳細 136

6インタフェースおよびルーティング 139

6.1インタフェース 139
6.1.1インタフェース 140
6.1.1.1自動インタフェースネットワーク定義 141
6.1.1.2インタフェースタイプ 141
6.1.1.33G/UMTS 142
6.1.1.4イーサネット標準 144
6.1.1.5イーサネットVLAN 147
6.1.1.6ケーブルモデム(DHCP) 149
6.1.1.7DSL(PPPoE) 151
6.1.1.8DSL(PPPoA/PPTP) 153
6.1.1.9モデム(PPP) 155
6.1.2追加アドレス 157
6.1.3リンクアグリゲーション 158
6.1.4アップリンクバランシング 159
6.1.5マルチパスルール 162
6.1.6ハードウェア 164
6.2ブリッジング 165
6.2.1ステータス 166
6.2.2詳細 168
6.3スタティックルーティング 168
6.3.1標準スタティックルート 169
6.3.2ポリシルート 170
6.4ダイナミックルーティング(OSPF) 172
6.4.1グローバル 173
6.4.2エリア 174
6.4.3インタフェース 176

6.4.4メッセージダイジェスト 178
6.4.5デバッグ 178
6.4.6詳細 179
6.5IPv6 180
6.5.1グローバル 180
6.5.2プレフィックス通知 181
6.5.36to4 182
6.5.4トンネルブローカ 183
6.6サービス品質(QoS) 184
6.6.1ステータス 184
6.6.2トラフィックセレクタ 186
6.6.3帯域幅プール 190
6.7マルチキャストルーティング(PIM-SM) 192
6.7.1グローバル 193
6.7.2インタフェース 194
6.7.3RPルータ 195
6.7.4ルート 196
6.7.5詳細 198
6.8アップリンクモニタリング 198
6.8.1グローバル 198
6.8.2アクション 199
6.8.3詳細 200

7ネットワークサービス 201

7.1DNS 201
7.1.1グローバル 201
7.1.2フォワーダ 202
7.1.3リクエストルーティング 202
7.1.4スタティックエントリ 203
7.1.5DynDNS 204
7.2DHCP 206
7.2.1サーバ 207
7.2.2リレー 209
7.2.3スタティックMAC/IPマッピング 210
7.2.4IPv4リーステーブル 211
7.2.5IPv6リーステーブル 212
7.3NTP 213

8ネットワークセキュリティ 215

8.1ファイアウォール 215
8.1.1ルール 215
8.1.2送受信国別ブロック 219

8.1.3ICMP 220
8.1.4詳細 221
8.2NAT 224
8.2.1マスカレード 224
8.2.2DNAT/SNAT 225
8.3侵入防御 228
8.3.1グローバル 228
8.3.2攻撃パターン 230
8.3.3DoS/フラッド防御 232
8.3.4ポートスキャン防御 234
8.3.5除外 235
8.3.6詳細 237
8.4サーバロードバランシング 239
8.4.1負荷分散ルール 239
8.5VoIP 242
8.5.1SIP 242
8.5.2H.323 244
8.6詳細 245
8.6.1汎用プロキシ 245
8.6.2SOCKSプロキシ 246
8.6.3IDENTリバースプロキシ 248

9Webセキュリティ 249

9.1Webフィルタリング 250
9.1.1グローバル 250
9.1.2アンチウイルス/マルウェア 254
9.1.3URLフィルタリング 256
9.1.4URLフィルタリングカテゴリ 260
9.1.5除外 261
9.1.6詳細 264
9.1.7HTTPS CA 269
9.2Webフィルタプロファイル 273
9.2.1概要 274
9.2.2プロキシプロファイル 275
9.2.3フィルタ割り当て 279
9.2.4フィルタアクション 280
9.2.5親プロキシ 284
9.3アプリケーションコントロール 285
9.3.1ネットワークの可視性 286
9.3.2アプリケーションコントロールルール 286
9.3.3詳細 289

9.4FTP 290
9.4.1グローバル 290
9.4.2アンチウイルス 291
9.4.3除外 293
9.4.4詳細 294
10メールセキュリティ 297
10.1SMTP 297
10.1.1グローバル 297
10.1.2ルーティング 298
10.1.3アンチウイルス 301
10.1.4アンチスパム 305
10.1.5除外 311
10.1.6リレー 313
10.1.7詳細 316
10.2SMTPプロファイル 319
10.3POP3 325
10.3.1グローバル 325
10.3.2アンチウイルス 326
10.3.3アンチスパム 328
10.3.4除外 330
10.3.5詳細 332
10.4暗号化 336
10.4.1グローバル 339
10.4.2オプション 341
10.4.3内部ユーザ 342
10.4.4S/MIME認証局 344
10.4.5S/MIME証明書 346
10.4.6OpenPGP公開鍵 347
10.5隔離レポート 349
10.5.1グローバル 350
10.5.2除外 352
10.5.3詳細 353
10.6メールマネージャ 355
10.6.1メールマネージャウィンドウ 356
10.6.1.1SMTP/POP3隔離 357
10.6.1.2SMTPスプール 358
10.6.1.3SMTPログ 359
10.6.2グローバル 360
10.6.3設定 362
11ワイヤレスセキュリティ 365

11.1グローバル設定 365
11.1.1グローバル設定 366
11.1.2詳細 367
11.2ワイヤレスネットワーク 369
11.3アクセスポイント 372
11.3.1アクセスポイントおよびSSIDグルーピング 373
11.4ワイヤレスクライアント 375

12Webアプリケーションセキュリティ 377

12.1Webアプリケーションファイアウォール 377
12.1.1グローバル 377
12.1.2仮想Webサーバ 378
12.1.3リアルWebサーバ 380
12.1.4ファイアウォールプロファイル 381
12.1.5除外 385
12.1.6詳細 386
12.2認証管理 386
12.2.1証明書 386
12.2.2認証局 387
12.2.3失効リスト 387
12.2.4詳細 387

13REDマネジメント 389

13.1概要 390
13.2グローバル設定 390
13.3デバイス設定 391
13.4導入ヘルパ 394

14ログ管理 397

14.1概要 397
14.2ログ管理インタフェース 398
14.2.1ダッシュボード 399
14.2.2グラフ 401
14.2.3イベント 402
14.2.4デバイス 403
14.2.5設定 404
14.2.6レポート 406
14.3ログ転送 407
14.4デバイス設定 407

15サイト間VPN 409

15.1IPsec 410
15.1.1接続 412

15.1.2リモートゲートウェイ 414
15.1.3ポリシ 417
15.1.4ローカルRSA鍵 421
15.1.5詳細 423
15.1.6デバッグ 426
15.2SSL 426
15.2.1接続 427
15.2.2設定 430
15.2.3詳細 432
15.3証明書管理 434
15.3.1証明書 434
15.3.2認証局 437
15.3.3失効リスト 439
15.3.4詳細 439

16リモートアクセス 441

16.1SSL 442
16.1.1グローバル 442
16.1.2設定 444
16.1.3詳細 445
16.2PPTP 447
16.2.1グローバル 448
16.2.2iOSデバイス 450
16.2.3詳細 451
16.3L2TP over IPsec 451
16.3.1グローバル 452
16.3.2iOSデバイス 455
16.3.3詳細 456
16.4IPsec 456
16.4.1接続 459
16.4.2ポリシ 461
16.4.3詳細 465
16.4.4デバッグ 468
16.5Cisco VPN Client 468
16.5.1グローバル 469
16.5.2iOSデバイス 470
16.5.3デバッグ 472
16.6詳細 472
16.7認証管理 473
16.7.1証明書 473
16.7.2認証局 474

16.7.3失効リスト ... 474
16.7.4詳細 ... 474

17ログおよびレポーティング 475

17.1ログファイルの閲覧 ... 477
17.1.1今日のログファイル ... 477
17.1.2アーカイブログファイル ... 478
17.1.3ログファイルの検索 ... 479
17.2ハードウェア ... 479
17.2.1デイリー ... 480
17.2.2ウィークリー ... 482
17.2.3マンスリー ... 482
17.2.4イヤリー ... 482
17.3ネットワーク使用状況 ... 482
17.3.1デイリー ... 483
17.3.2ウィークリー ... 483
17.3.3マンスリー ... 484
17.3.4イヤリー ... 484
17.3.5帯域幅使用状況 ... 484
17.4ネットワークセキュリティ ... 486
17.4.1デイリー ... 486
17.4.2ウィークリー ... 487
17.4.3マンスリー ... 487
17.4.4イヤリー ... 488
17.4.5ファイアウォール ... 488
17.4.6IPS ... 488
17.5Webセキュリティ ... 489
17.5.1Web使用状況レポート ... 489
17.5.2検索エンジンレポート ... 493
17.5.3部門 ... 495
17.5.4スケジュールされたレポート ... 496
17.5.5アプリケーションコントロール ... 497
17.5.6非匿名化 ... 498
17.6メールセキュリティ ... 499
17.6.1使用状況グラフ ... 499
17.6.2メール使用状況 ... 500
17.6.3ブロックされたメール ... 500
17.6.4非匿名化 ... 501
17.7リモートアクセス ... 502
17.7.1アクティビティ ... 502
17.7.2セッション ... 502

17.8Webアプリケーションファイアウォール..... 504
17.8.1使用状況グラフ..... 504
17.8.2詳細..... 504
17.9エグゼクティブレポート..... 505
17.9.1レポートを見る(View Report)..... 505
17.9.2アーカイブエグゼクティブレポート(Archived Executive Reports)..... 505
17.9.3設定..... 505
17.10ログ設定..... 506
17.10.1ローカルログ..... 506
17.10.2リモートSyslogサーバ..... 508
17.10.3リモートログファイルアーカイブ..... 510
17.11レポーティング設定..... 513
17.11.1設定..... 513
17.11.2除外..... 515
17.11.3匿名化..... 515

18サポート 517

18.1マニュアル..... 517
18.2印刷可能設定..... 518
18.3サポートのお問い合わせ先..... 519
18.4ツール..... 519
18.4.1Pingチェック..... 519
18.4.2Traceroute..... 520
18.4.3DNSルックアップ..... 522
18.5詳細..... 522
18.5.1プロセスリスト..... 523
18.5.2ローカルネットワークコネクション..... 523
18.5.3ルーティングテーブル..... 523
18.5.4インタフェーステーブル..... 523
18.5.5コンフィグダンプ..... 523
18.5.6REFの解決..... 524

19ログオフ 525

1 インストール

このセクションは、ネットワークへのAstaro Security Gatewayのインストールとセットアップについての情報を提供します。Astaro Security Gatewayのインストールは、2つのステップで行います。まず、ソフトウェアをインストールします。次に、基本システム設定を行います。ソフトウェアのインストールに必要な初期セットアップは、コンソールベースのインストールメニューで行います。内部設定は、管理ワークステーションで、Astaro Security GatewayのWebベースの管理用インタフェースであるWebAdminを使用して実行できます。インストールを開始する前に、ハードウェアがシステムの最低要件を満たしていることを確認してください。

注 - Astaro Security Gatewayアプライアンスを導入している場合、次のセクションをスキップして、*基本設定*のセクションに直接進むことができます。この理由は、すべてのAstaro Security GatewayアプライアンスはASGソフトウェアがプレインストールされた状態で出荷されるためです。

この章には次のトピックが含まれます。

- 参考資料
- システム要件
- インストール手順
- 基本設定
- バックアップリストア

1.1 参考資料

インストールを始める前に、Astaro Security Gateway製品の設定の一助となる以下のマニュアルを読むことをお勧めします。いずれのマニュアルも、Astaro Security Gateway アプライアンス装置に同梱されています。また、以下でもご利用いただけます: Astaroナレッジベース:

- クイックスタートガイドハードウェア(Quick Start Guide Hardware)
- 取扱説明書(Operating Instructions)

1.2 システム要件

ASGのインストールおよび使用のための最低限のハードウェア要件は以下のとおりです。

- **プロセッサ**: Pentium 4(1.5GHz)(あるいは互換のもの)
- **メモリ**: 1 GBRAM
- **HDD**: 20GB IDEまたはSCSIハードディスクドライブ
- **CD-ROMドライブ**: ブート(起動)可能なIDE 、またはSCSI CD-ROMドライブ
- **NIC**: 2枚以上のPCIイーサネットネットワークインタフェースカード
- **NIC**(オプション):1枚のハートビート対応PCI イーサネットネットワークインタフェースカード。高可用性システムでは、プライマリシステムとセカンダリシステムが、いわゆるハートビート要求を介して互いに通信します。高可用性システムをセットアップする場合は、両方のユニットにハートビート対応のネットワークインタフェースカードを装備する必要があります。
- **USB**(オプション):UPSUSB通信用に1つのUSBポート
- **スイッチ**(オプション):ネットワークセグメントの接続(およびその間の選択)を行うネットワークデバイス。このスイッチはジャンボフレームをサポートすることが必要です。

AstaroではASGソフトウェアのバグフィックスおよび拡張機能が含まれています。*ハードウェア互換性リスト*(HCL)は次からご利用いただけます: Astaroナレッジベース.ASGソフトウェアのインストールと使用でエラーの発生を防止するために、HCLにリストされたハードウェアのみを使用してください。WebAdminへのアクセスに使用されるクライアントPCに必要なハードウェアおよびソフトウェアの条件を以下に示します。

- **プロセッサ**: クロック周波数:1GHz以上
- **ブラウザ**: Firefox 2(推奨)あるいはMicrosoft Internet Explorer6または7。JavaScriptを有効にする必要があります。さらに、ASGの内部ネットワークカードのIPアドレス(eth0)にプロキシを使用しないようにブラウザを設定する必要があります。

注 –Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの【*インターネットオプション*】>>【*セキュリティ*】で設定します。さらに、Internet Explorer 7を使用する場合は、【*信頼済みサイトゾーン*】で【*ファイルのダウンロード時に自動的にダイアログを表示*】を選択します。

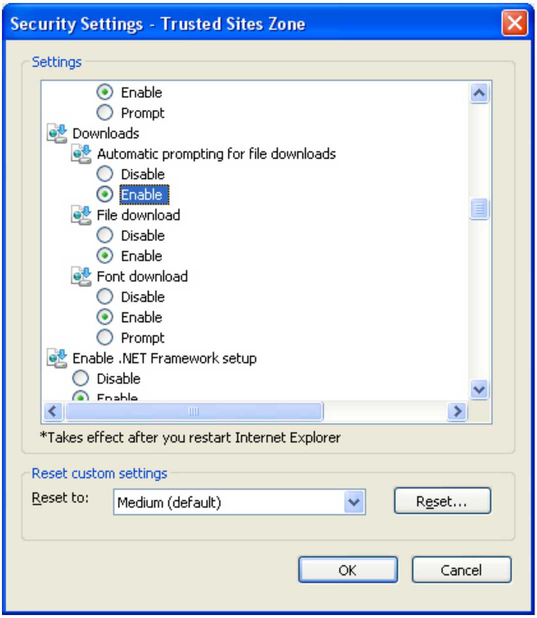


図1 IE7 セキュリティ設定信頼済みサイト ゾーン

1.2.1 UPSデバイスのサポート

無停電電源装置(UPS)デバイスは、公共の電力が利用できない場合に、別個の電源から接続した機器に電力を供給して給電を維持します。Astaro Security Gateway は、MGE UPS SystemsおよびAPCのUPSデバイスをサポートしています。UPSデバイスとAstaro Security Gateway の通信はUSB インタフェースで行います。

UPSデバイスがバッテリオペレーションを始動すると、管理者に通知が送信されます。停電が長期間続いてUPSデバイスの電圧が限界値に近づいた場合は、管理者に別のメッセージが送信されます。そして、Astaro Security Gateway は自動的にシャットダウンします。

注 – 当製品にUPSデバイスを接続するときは、UPSデバイスの使用説明書をお読みください。Astaro Security Gateway. USBインタフェースを介してブート(起動)すると、ASGはUPSデバイスを認識します。USBインタフェースを相互に接続してからAstaro Security Gateway をブートしてください。

1.2.2RAIDサポート

RAID(*Redundant Array of Independent Disks*)とは、複数のハードドライブを使用してドライブ間でデータを共有あるいは複製するデータストレージ技術です。RAIDシステムが検出されてダッシュボードに正しく表示されるようにするには、当製品でサポートされるRAIDコントローラを使用することが必要です。Astaro Security Gateway.サポートされているRAIDコントローラを確認するには、HCLをチェックしてください。HCLはAstaroナレッジベースで提供されています。「HCL」を検索用語として使用して、該当するページを探してください。

1.3インストール手順

次に、Astaro Security Gatewayソフトウェアのインストールプロセスを順を追って説明します。

インストールを始める前に、次のアイテムがお手元にあることを確認してください。

- Astaro Security Gateway CD-ROM
- Astaro Security Gatewayのライセンスキー

セットアッププログラムがシステムのハードウェアをチェックしてから、PCにソフトウェアをインストールします。

1.3.1インストール中の主な機能

メニューのナビゲーションには、次のキーを使用します(画面の下部にも追加のキー機能がリストされています)。

- F1:コンテキストに応じたヘルプ画面が表示されます。
- カーソルキー:これらのキーを使用して、テキストボックス間をナビゲーションします(たとえば、ライセンス条件や、キーボードレイアウトの選択時)。
- Tabキー:テキストボックス、リスト、ボタンを前後に移動します。
- Enterキー:入力した情報が確定され、インストールが次のステップに進みます。
- Spaceキー:アスタリスク(*)の付いたオプションを選択または選択解除します。
- Alt-F2:インストールコンソールに切り替えます。
- Alt-F4:ログに切り替えます。

- Alt F1：インタラクティブバッシュシェルに切り替えます。
- Alt-F1：メインのインストール画面に戻ります。

1.3.2インストール中の特別なオプション

一部の画面には追加のオプションがあります。

ログの閲覧(View Log)：インストールログを開きます。

サポート(Support)：サポートダイアログ画面を開きます。

USBスティックへ(To USB Stick)：インストールログをzipファイルとしてUSBスティックへ書き込みます。このオプションを確定する前に、必ずUSBスティックを差し込んでください。このzipファイルは、インストールでの問題をAstaroサポートチームなどが解決する際に使用されます。

戻る(Back)：前の画面に戻ります。

キャンセル(Cancel)：インストールの中止を確認するダイアログウィンドウが開きます。

ヘルプ(Help)：コンテキストに応じたヘルプ画面が開きます。

1.3.3インストール中 Astaro Security Gateway

1. **CD-ROMドライブからPCをブートします。**
   インストール開始画面が表示されます。

   注 - いつでもF1を押してヘルプメニューを利用することができます。開始画面でF3を押すと、トラブルシューティングの画面が開きます。

2. **Enterを押します。**
   *【開始(Introduction)】*画面が表示されます。

3. ***【インストール開始(Start Installation)】*を選択します。**
   *【ハードウェア検出(Hardware Detection)】*画面が表示されます。

   ソフトウェアが次のハードウェアコンポーネントをチェックします。

   - CPU
   - ハードディスクドライブのサイズと型
   - CD-ROMドライブ

- ネットワークインタフェースカード
- IDE、またはSCSIコントローラ

システムが最低要件を満たしていない場合、エラーが報告され、インストールは中止されます。

ハードウェア検出が完了すると、【*検出されたハードウェア(Detected Hardware)*】画面が参考として表示されます。

4. **Enterを押します。**
【*キーボード選択(Select Keyboard)*】画面が表示されます。

5. **キーボードのレイアウトを選択します。**
カーソルキーを使用してキーボードレイアウト(例:*English (UK)*)を選択し、Enterを押して続行します。

【*タイムゾーン選択(Select Timezone)*】画面が表示されます。

6. **エリアを選択します。**
カーソルキーを使用してエリア(例:*Europe*)を選択し、Enterを押して続行します。

7. **タイムゾーンを選択します。**
カーソルキーを使用してタイムゾーン(例:*London*)を選択し、Enterを押して続行します。

【*日付と時刻(Date and Time)*】画面が表示されます。

8. **日付と時刻を設定します。**
日付と時刻が正しくない場合、ここで変更できます。Tabキーとカーソルキーを使用して、テキストボックス間を切り替えます。【*ホストクロックはUTC(Host Clock is UTC)*】オプションの選択を解除するには、Spaceキーを押します。無効なエントリは却下されます。設定をEnterキーで確認します。

【*管理インタフェース選択(Select Admin Interface)*】画面が表示されます。

9. **内部ネットワークカードを選択します。**
WebAdminツールを使用してAstaro Security Gatewayの残りの設定を行う場合、内部ネットワークカード(eth0)とするネットワークインタフェースカードを選択します。リストから使用可能なネットワークカードを1つ選択し、Enterキーで選択を確認します。

注 - アクティブな接続があるインタフェースには「*LINK*」という言葉が付いています。

【*ネットワーク設定(Network Configuration)*】画面が表示されます。

10. **管理ネットワークインタフェースを設定します。**
管理ネットワークインタフェースとする内部インタフェースのIPアドレス、ネットワークマスク、ゲートウェイを定義します。デフォルト値は以下のとおりです。

アドレス(Address):192.168.2.100

ネットマスク(Netmask):255.255.255.0

ゲートウェイ(Gateway): なし

ネットマスクで定義されたサブネット外にあるワークステーションからWebAdminインタフェースを使用したい場合のみ、ゲートウェイ値を変更する必要があります。ゲートウェイ自体がサブネット内にある必要があります。[1]

設定をEnterキーで確認します。

CPUが64ビットをサポートしている場合、【*64ビットカーネルのサポート(64 Bit Kernel Support)*】画面が表示されます。サポートしていない場合、続いて【*Enterprise Toolkit*】画面が表示されます。

11. **64ビットカーネルのインストール(Install the 64-bit kernel)**
【*はい(Yes)*】を選択すると64ビットカーネルが、【*いいえ(No)*】をインストールすると32ビットカーネルがインストールされます。

【*Enterprise Toolkit*】画面が表示されます。

12. **Enterprise Toolkitのインストールに同意します。**
Enterprise ToolkitはAstaroソフトウェアから構成されています。Open Sourceソフトウェアのインストールのみを決定できます。ただし、Astaro Security Gatewayの全機能を使用するためには、Enterprise Toolkitもインストールすることをお勧めします。

Enterを押して両方のソフトウェアパッケージをインストールするか、【*いいえ(No)*】を選択してOpen Sourceソフトウェアのみをインストールします。

【*インストール: パーティショニング(Installation: Partitioning)*】画面が表示されます。

---

[1]たとえば、255.255.255.0というネットワークマスクを使用している場合、サブネットはアドレスの最初の3オクテットで定義されます。この場合は、192.168.2です。管理コンピュータのIPアドレスが192.168.10.5である場合、同じサブネット上にないため、ゲートウェイが必要になります。ゲートウェイルータは、192.168.2サブネット上にインタフェースが必要であり、管理コンピュータに連絡できなければなりません。この例では、ゲートウェイのIPアドレスは192.168.2.1とします。

13. **警告メッセージを確認してインストールを開始します。**
警告は注意して読んでください。確認後、PCにすでに存在するすべてのデータが削除されます。

設定を変更するには、【*戻る(Back)*】を選択します。

> **警告 -** インストールプロセスを行うと、ハードディスクドライブ上のすべてのデータが削除されます。

ソフトウェアのインストールプロセスには最大2、3分かかる可能性があります。

【*インストール完了(Installation Finished)*】画面が表示されます。

14. **CD-ROMを取り出して、内部ネットワークに接続し、システムをリブートします。**
インストールプロセスが完了したら、ドライブからCD-ROMを取り出して、`eth0`ネットワークカードを内部ネットワークに接続します。内部ネットワークカード(`eth0`)を除き、ネットワークカードの順序は、通常PCI IDおよびカーネルドライバによって決定されます。ハードウェア構成を変更すると(特にネットワークカードを取り外した場合や追加した場合など)、ネットワードカード名の順序も変わる可能性があります。

次に、インストール画面でEnterを押し、ASGをリブートします。ブートプロセス中に、内部ネットワークカードのIPアドレスが変わります。このとき、インストールルーチンコンソール(Alt+F1)に、「eth0にIPなし(No IP on eth0)」というメッセージが表示されます。

Astaro Security Gatewayのリブート後(ハードウェアによっては、このプロセスは数分かかります)、`eth0`インタフェースのIPアドレスをpingし、このアドレスが到達可能であることを確認します。接続できない場合、次のいずれかの問題が発生していないかチェックしてください。

- Astaro Security GatewayのIPアドレスが誤っている。
- クライアントコンピュータのIPアドレスが正しくない。
- クライアントのデフォルトゲートウェイが正しくない。
- 正しくないネットワークカードにネットワークケーブルが接続されている。
- すべてのネットワークカードが同じハブに接続されている。

1.4基本設定

インストールの2番目のステップはWebAdminで行います。これは、Astaro Security GatewayのWebベースの管理インタフェースです。基本システム設定の前に、Astaro Security Gateway

をネットワークに統合する方法を計画しておく必要があります。どのような機能を提供するか(ブリッジモードと標準(ルーティング)モードのどちらで運用するか、インタフェース間でデータパケットの流れをどのようにコントロールするかなど)を決定する必要があります。ただし、Astaro Security Gateway は後でいつでも再設定できます。したがって、Astaro Security Gateway をネットワークに統合する方法をまだ計画していない場合でも、すぐに基本設定に着手することが可能です。

1. **ブラウザを起動して、WebAdminを開きます。**
   Astaro Security GatewayのURL(eth0のIPアドレス)を参照します。上記の設定例との整合性を保つために、これは`https://192.168.2.100:4444`とします(プロトコルがHTTPS であり、ポート番号が4444であることに注意してください)。

   設定例と異なり、各Astaro Security Gatewayアプライアンスの出荷時は次のデフォルト設定になっています。

   - **インタフェース(Interfaces)**: 内部ネットワークインタフェース(eth0)
   - **IPアドレス(IP address)**: 192.168.0.1
   - **ネットワークマスク(Network mask)**: 255.255.255.0
   - **デフォルトゲートウェイ(Default gateway)**: なし

   任意のAstaro Security GatewayアプライアンスのWebAdminにアクセスするには、代わりに次のURLを入力します。

   `https://192.168.0.1:4444`

   認証および暗号化された通信を提供するために、Astaro Security Gateway には、自己署名済みのセキュリティ証明書が含まれています。この証明書は、WebAdminへのHTTPS接続が確立するとWebブラウザに対して提供されます。証明書の有効期間を確認できない場合、ブラウザはセキュリティ警告を表示します。証明書に同意すると、最初のログインページが表示されます。

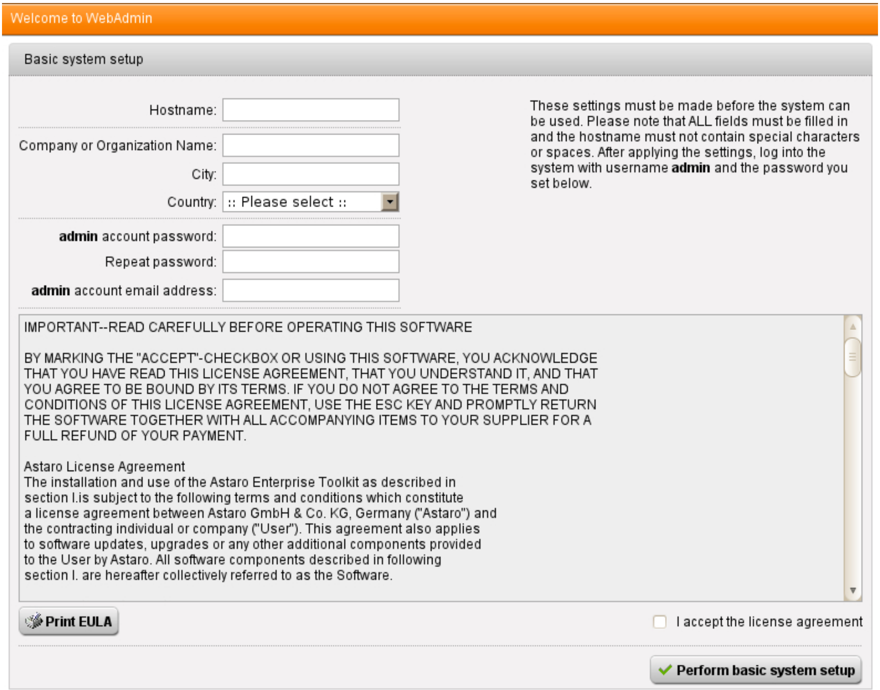


図2 WebAdmin：初期ログインページ

2. **【基本システム設定(Basic System Setup)】フォームに記入します。**
   ここに表示されるテキストボックスに会社の情報を正確に入力します。さらに、管理者アカウントにパスワードと有効なEメールアドレスを指定します。ライセンス条件に同意する場合は、**【*基本システム設定の実行(Perform Basic System Setup)*】**ボタンをクリックしてログインを続行します。基本システム設定の実行中、多数の証明書と認証局が作成されます。

   - **WebAdmin CA**：WebAdmin証明書に署名したCA(*「マネジメント」*>>*「WebAdminの設定」*>>*「HTTPS証明書」*を参照)。
   - **VPNに署名するCA(VPN Signing CA)**：VPN接続に使用されるデジタル証明書に署名するCA(*「サイト間VPN」*>>*「認証管理」*>>*「認証局」*を参照)。
   - **証明書を再生成(Re-generate WebAdmin Certificate)**：WebAdminのデジタル証明書(*「サイト間VPN」*>>*「証明書管理」*>>*「証明書」*を参照)。

- **ローカルX.509証明書(Local X.509 Certificate)**:VPN接続に使用される、Astaro Security Gatewayのデジタル証明書(*「サイト間VPN」>>「証明書管理」>>「証明書」*を参照)。

ログインページが表示されます。(ただし、入力した値に基づいて証明書が変更されているため、一部のブラウザでは、さらにセキュリティ警告が表示される場合もあります。)

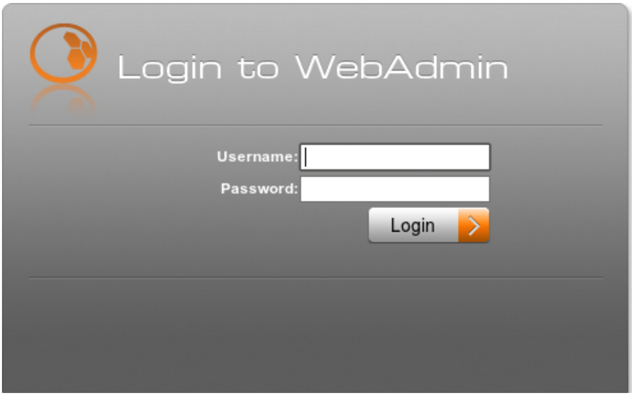


図3 WebAdmin:通常のログインページ

3. **WebAdminにログインします。**
*【ユーザ名(Username)】*フィールドに「admin」と入力し、前の画面で指定したパスワードを入力します。

 初期設定プロセスをガイドする設定ウィザードが表示されます。ウィザードのステップに従い、Astaro Security Gatewayの基本設定を行います。

 バックアップファイルがある場合、代わりにこのバックアップファイルをリストアすることもできます(「*バックアップリストア*」のセクションを参照)。

 あるいは、(ウィザードの任意のステップで)*【キャンセル(Cancel)】*をクリックし、安全にウィザードを終了することもできます(Astaro Security GatewayをWebAdminで直接設定したい場合など)。いつでも*【終了(Finish)】*をクリックし、そこまでの設定を保存してウィザードを終了できます。

4. **ライセンスをインストールします。**
購入したライセンス(テキストファイル)をアップロードするには、フォルダのアイコンをクリックします。*【次へ(Next)】*をクリックしてライセンスをインストールします。ライセンスを購入していない場合、*【次へ(Next)】*をクリックして、製品に組み込まれた30日間のトライアルライセンス

を使用してください。Astaro Security Gatewayに搭載されたすべての機能が有効になります。

5. **内部ネットワークインタフェースを設定します。**
内部ネットワークインタフェース(*eth0*)に対して表示された設定を確認します。このインタフェースの設定は、ソフトウェアのインストール時に提供した情報に基づいています。さらに、チェックボックスをオンにして、Astaro Security Gatewayが内部インタフェースでDHCPサーバとして機能するように設定することができます。

注 – 内部インタフェースのIPアドレスを変更する場合、ウィザード終了後に新しいIPアドレスを使用してWebAdminに接続し直す必要があります。

6. **外部インタフェースのアップリンクタイプを選択します。**
外部ネットワークカードで使用するアップリンク/インターネット接続の接続タイプを選択します。インタフェースのタイプとその設定は、どのような種類のインターネット接続を使用するかによって異なります。【*次へ(Next)*】をクリックします。

Astaro Security Gatewayにアップリンクがないか、今すぐ設定したくない場合には、【*インターネットアップリンクタイプ(Internet Uplink Type)*】入力ボックスを空欄のまま残します。インターネットアップリンクを設定すると、内部ネットワークからインターネットへの接続用にIP マスカレーディングが自動設定されます。

【*スタティックIPアドレスによる標準イーサネットインタフェース(Standard Ethernet Interface with Static IP Address)*】を選択する場合、*デフォルトゲートウェイ*の指定はオプションです。テキストボックスを空欄のままにすると、インストール時のデフォルトゲートウェイ設定が維持されます。【*次へ(Next)*】をクリックして、残りの各ステップをスキップすることができます。スキップした設定は、後でWebAdminで設定・変更できます。

7. **基本的なファイアウォール設定を行います。**
ここで、インターネットで許可するサービスのタイプを選択できます。【*次へ(Next)*】をクリックして設定を確認します。

8. **基本的な侵入防止設定を行います。**
ここで、複数のオペレーションシステムとデータベースに対する侵入防止を設定できます。【*次へ(Next)*】をクリックして設定を確認します。

9. **インスタントメッセージングとP2P用の設定を行います。**
ブロックするインスタントメッセージやピアツーピアプロトコルを選択できます。【*次へ(Next)*】をクリックして設定を確認します。

10. **Webセキュリティ設定を行います。**
ここで、Webトラフィックに対してウイルスやスパイウェアのスキャンを行う必要があるかどうかを選択できます。さらに、特定のカテゴリに属するWebページのブロックを選択できます。【*次へ(Next)*】をクリックして設定を確認します。

11. **メールセキュリティ設定を行います。**
ここでは、最初のチェックボックスにチェックを入れて、POP3プロキシを有効にすることができます。また、2つ目のチェックボックスをオンにして、ASGをインバウンドSMTPリレーとして有効にすることができます。内部メールサーバのIPアドレスを入力し、SMTPドメインをルートに追加します。【*次へ(Next)*】をクリックして設定を確認します。

12. **設定を確認します。**
設定のサマリが表示されます。【*終了(Finish)*】をクリックして確認するか、【*戻る(Back)*】をクリックして変更します。これらは後でWebAdminで変更することもできます。

【*終了(Finish)*】をクリックすると設定は保存され、ユーザはWebAdminのダッシュボードにリダイレクトされます。ここで、Astaro Security Gatewayユニットの最も重要なシステムステータス情報が表示されます。

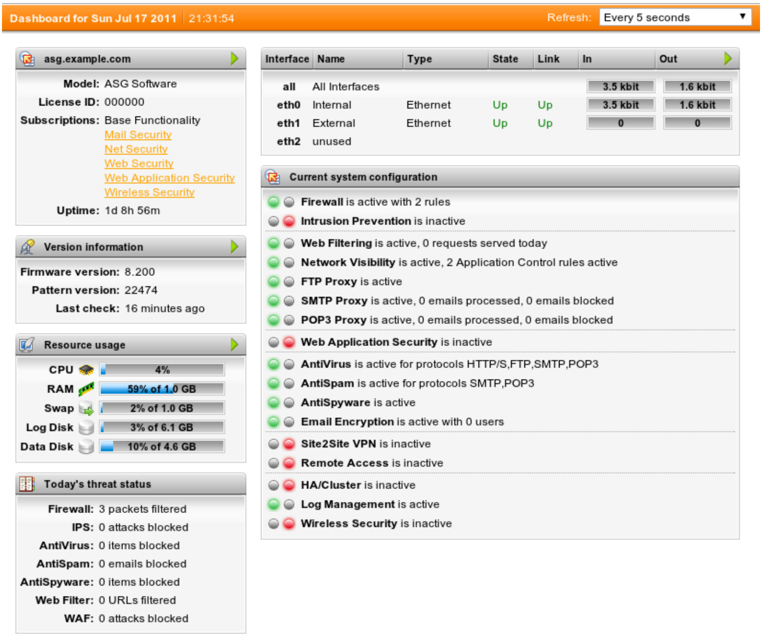


図4　WebAdmin：ダッシュボード

これらのステップの実行中に問題が発生した場合は、Astaro Security Gatewayサプライヤのサポート部門にお問い合わせください。次のWebサイトでも詳細情報を提供しています。

- Astaroサポートフォーラム
- Astaroナレッジベース

1.5バックアップリストア

WebAdmin設定ウィザード(「基本設定」セクションを参照)を使用すると、基本設定プロセスをすべて実行する代わりに、既存のバックアップファイルをリストアすることができます。以下の手順に従ってください。

1. **設定ウィザードで*【既存のバックアップファイルのリストア(Restore existing backup file)】*を選択します。**

設定ウィザードで【*既存のバックアップファイルのリストア(Restore existing backup file)*】を選択し、【*次へ(Next)*】をクリックします。

アップロードページが表示されます。

2. **バックアップをアップロードします。**
   フォルダアイコンをクリックし、リストアするバックアップファイルを選択して、【*アップロード開始(Start Upload)*】をクリックします。

3. **バックアップをリストアします。**
   【*終了(Finish)*】をクリックしてバックアップをリストアします。

重要 - 後で設定ウィザードを使用することはできません。

バックアップのリストアが成功すると、ログインページにリダイレクトされます。

2WebAdmin

WebAdminはWebベースの管理インタフェースで、ここでは当製品のあらゆる局面の設定を行うことができます。Astaro Security Gateway. WebAdminはメニューとページで構成され、それらの多くには複数のタブが含まれています。画面左側のメニューには、Astaro Security Gatewayの機能が論理的に構成されています。【*ネットワーク(Network)*】などのメニュー項目を選択すると、それが拡大してサブメニューが表示されたり関連ページが開きます。メニュー項目の中には、関連ページがないものもあります。前に選択したメニューまたはサブメニュー項目のページは、そのまま表示されます。サブメニュー項目のいずれかを選択すると、それによって最初のタブの関連ページが開きます。

この管理ガイドの手順に従ってメニュー項目、サブメニュー項目、およびタブを指定すると、ページが開きます(例:【*インタフェースおよびルーティング(Interfaces & Routing)*】>>【*インタフェース(Interfaces)*】>>【*ハードウェア(Hardware)*】タブ)。

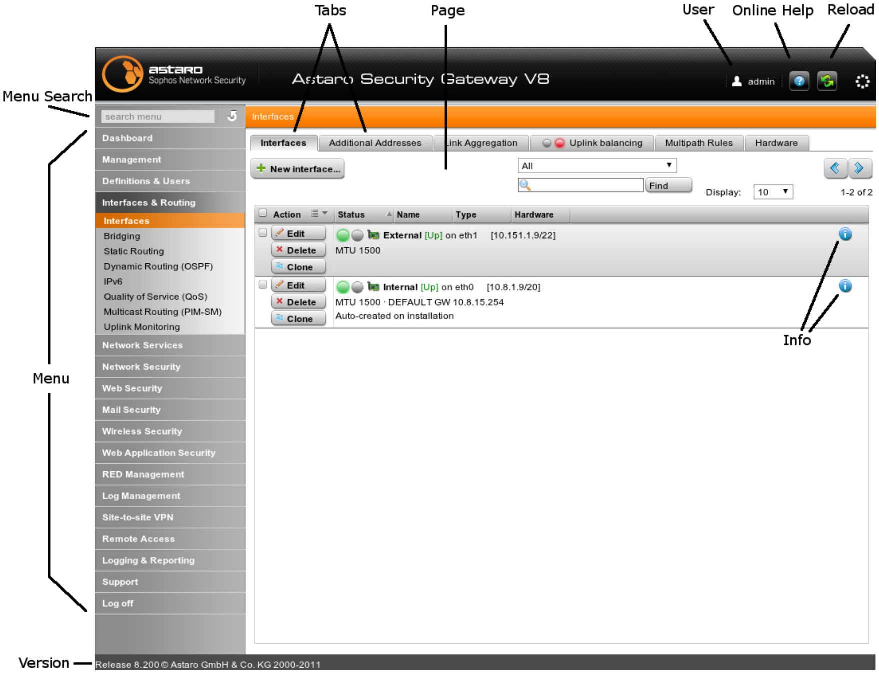


図5 WebAdmin:概要

2.1WebAdminメニュー

WebAdminメニューは、Astaro Security Gatewayのすべての設定オプションへのアクセスを提供します。したがって、特定パラメータの設定にコマンドラインインタフェースを使用する必要はありません。

- **ダッシュボード(Dashboard)**:ダッシュボードは、Astaro Security Gatewayユニットの現在の操作状況をグラフィカルに表示します。
- **マネジメント(Management)**: 基本的なシステム設定、WebAdmin設定、およびAstaro Security Gatewayユニットの設定に関するすべての設定を構成します。
- **定義およびユーザ(Definitions & Users)**:Astaro Security Gatewayユニットで使用するネットワーク、サービス、期間定義、およびユーザアカウント、ユーザグループ、外部認証サーバを構成します。
- **インタフェースおよびルーティング(Interfaces & Routing)**: ネットワークインタフェースおよびルーティングオプションなどのシステム機能を設定します。
- **ネットワークサービス(Network Services)**: DNSやDHCPなどのネットワークサービスを設定します。
- **ネットワークセキュリティ(Network Security)**: ファイアウォールルール、VoIP、侵入防止設定などの基本的なネットワークセキュリティ機能を設定します。
- **Webセキュリティ(Web Security)**:Astaro Security GatewayユニットのWebフィルタおよびアプリケーションコントロール、ならびにFTPプロキシを設定します。
- **メールセキュリティ(Mail Security)**:Astaro Security Gateway ユニットのSMTPおよびPOP3プロキシ、ならびにEメールの暗号化を設定します。
- **ワイヤレスセキュリティ(Wireless Security)**: ゲートウェイのワイヤレスアクセスポイントを設定します。
- **Webアプリケーションセキュリティ(Web Application Security)**: WebサーバをクロスサイトスクリプティングやSQLインジェクションなどの攻撃から防御します。
- **REDマネジメント(RED Management)**: RED(Remote Ethernet device)アプライアンスを設定します。
- **ログ管理(Log Management)**: ログファイルを集中管理するストレージを設定します。
- **サイト間VPN(Site-to-site VPN)**: サイト間VPN(バーチャルプライベートネットワーク)を設定します。

- **リモートアクセス(Remote Access)**：Astaro Security Gatewayユニットへのリモートアクセス VPN接続を設定します。
- **ログおよびレポーティング(Logging & Reporting)**：Astaro Security Gatewayユニットの使用状況に関するログメッセージと統計を表示し、ログおよびレポーティングに関する設定を構成します。
- **サポート(Support)**：Astaro Security Gatewayユニットで利用できるサポートツールにアクセスします。
- **ログオフ(Log Off)**: ユーザインタフェースからログアウトします。

メニューの検索

メニュー上部に検索ボックスがあります。ここではキーワードについてメニューを検索し、特定のトピックに関するメニューを容易に検索できます。検索機能はメニュー名を検索しますが、非表示の索引付けされた別名やキーワードも検索できます。

検索ボックスに入力を開始するとすぐに、関連するメニュー項目のみが自動的に表示されます。検索ボックスはそのままにして、該当すると予想されるメニュー項目をクリックしてください。少なくなったメニュー項目はそのまま残り、その隣りのリセットボタンをクリックするまで検索結果が表示されます。

ヒント – キーボードショートカット`CTRL+Y`で検索ボックスにフォーカスすることができます。

2.2ボタンバー

WebAdminの右上隅にあるボタンから、次の機能にアクセスできます。

- **ユーザ/IPアドレス(User/IP Address)**: 現在ログインしているユーザと、WebAdminにアクセスしているIPアドレスを示します。
- **オンラインヘルプ(Online Help)**: すべてのメニュー、サブメニュー、タブにはオンラインヘルプ画面があり、WebAdminの現在ページのコントロールに関連するコンテキストに応じた情報や手順を提供します。

  注 - オンラインヘルプは、パターン更新によって更新されており、説明は常にAstaro Security Gatewayの最新バージョンに基づいているため、オンラインヘルプと現在インストールされているファームウェアの間にわずかな不整合が発生する場合があります。

- **リロード(Reload)**: すでに表示されているWebAdminページを再び要求する場合、必ず【*リロード(Reload)*】ボタンをクリックしてください。

> **注 -** ブラウザの「再読み込み」ボタンや「更新」ボタンは使用しないでください。これを行うと、WebAdminからログアウトすることになります。

2.3リスト

WebAdminの多くのページにはリストがあります。各リストの左にあるボタンを使用すると、アイテムの編集、削除、または複製が可能です(詳しくは「ボタンとアイコン」セクションを参照してください)。リストにアイテムを追加するには、【*新規...(New ...)*】ボタンをクリックします。ここで「...」は、作成中のオブジェクト(インタフェースなど)を示すプレースホルダです。ダイアログボックスが開き、新規オブジェクトのプロパティを定義することができます。

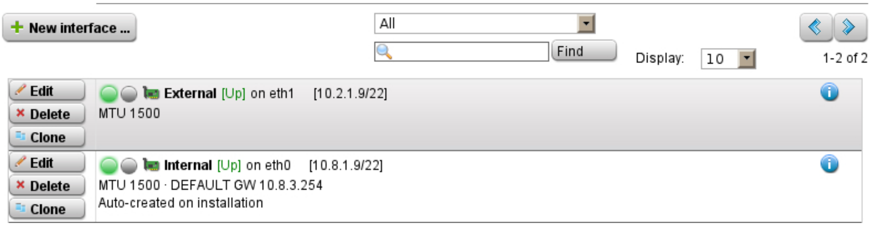


図6 WebAdmin:リストの例

それぞれのリストでは、タイプ別にすべてのアイテムをソートすることができます。さらに、検索ボックスを使用して、具体的なアイテムを検索することができます。検索文字列を入力し、【*検索(Find)*】をクリックします。

アイテムが11個以上含まれるリストは、複数ページに分割され、【>】(次へ)ボタンと【<】(前へ)ボタンを使用して移動することができます。ただし、この設定は【*ユーザ設定(User Preferences)*】タブで変更できます。

> **ヒント -** 情報アイコンをクリックすると、そのオブジェクトが使用されているすべての設定オプションが表示されます。

2.4ダイアログボックス

ダイアログボックスとは、特定の情報の入力を求めるためにWebAdminが使用する特別なウィンドウです。例として、*【インタフェース(Interfaces)】>>【ルーティング(Routing)】>>【スタティックルーティング(Static Routing)】*メニューで表示される、新しいスタティックルートを作成するためのダイアログボックスを示します。

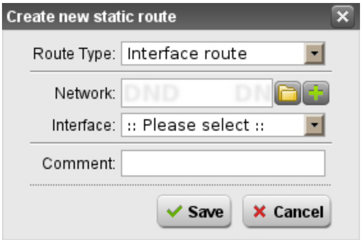


図7 WebAdmin:ダイアログボックスの例

各ダイアログボックスは、テキストボックス、チェックボックスなどの各種ウィジェットから構成されています。さらに、多くのダイアログボックスにはドラッグ&ドロップ機能があり、*DND*と記された特別な背景で識別されます。このようなボックスが表示された場合、ボックスにオブジェクトをドラッグすることができます。オブジェクトをドラッグする元の場所となるオブジェクトリストを開くには、テキストボックスのすぐ横にあるフォルダアイコンをクリックします。これにより、設定オプションに応じて、使用可能なネットワーク、インタフェース、ユーザ/グループ、またはサービスのリストが開きます。緑色の「+」アイコンをクリックすると、2つ目のダイアログボックスが開き、新しい定義を作成することができます。特定の設定で不要なウィジェットは、グレーアウト表示されます。これらのウィジェットを編集できる場合もありますが、効果はありません。

注 - WebAdminには、*【保存(Save)】*ボタンと*【適用(Apply)】*ボタンの両方が存在します。*【保存(Save)】*ボタンは、スタティックルートやネットワーク定義といったWebAdmin内のオブジェクトを作成または編集するときに使用します。常に、対応する*【キャンセル(Cancel)】*ボタンが用意されています。一方、*【適用(Apply)】*ボタンは、バックエンドで設定を確認し、速やかに有効化するために使用します。

2.5ボタンとアイコン

ここでは、WebAdminで使用されているボタンとアイコンの用途について説明します。

ボタン	意味
View	オブジェクトの詳細情報を示すダイアログウィンドウが表示されます。
Edit	オブジェクトのプロパティを編集するためのダイアログウィンドウが開きます。
Delete	オブジェクトを削除します。そのオブジェクトが他の箇所でまだ使用されている場合は、警告が表示されます。使用中のオブジェクトは削除できない場合があります。
Clone	同じ設定やプロパティで別のオブジェクトを作成するためのダイアログウィンドウが開きます。同じ設定を何度も繰り返し入力する必要なく、類似のオブジェクトを作成できます。

機能アイコン	意味
	情報: オブジェクトが使用されているすべての設定が表示されます。
	ステータス(Status): 機能を有効または無効にします。有効な場合は緑、無効な場合は赤、有効化する前に設定が必要な場合はアンバーとなります。
	フォルダ: 2種類の機能があります。(1) 左側にあるオブジェクトリストを開く(下のセクションを参照)。ここで適切なオブジェクトを選択できます。(2) ファイルのアップロード用のダイアログウィンドウを開く。
	プラス(+): 必要なタイプの新しいオブジェクトを追加するためのダイアログボックスが開きます。
	ゴミ箱: 現在の設定からオブジェクトを除去します。ただし、このオブジェクトは削除されるわけではありません。
	インポート: 複数のアイテムまたは行を持つテキストをインポートするためのダイアログウィンドウが開きます。複数のアイテムを個別に入力するのではなく、まとめて追加することができます(たとえば、URLブラックリストに大規模なブラックリストを追加する)。任意の場所からテキストをコピーし、CTRL+Vで貼り付けます。
	エクスポート: 既存のアイテムをすべてエクスポートするためのダイアログウィンドウが開きます。アイテムを区切るための区切り文字として、新しい行、コロン、コンマのいずれかを選択できます。アイテムをテキストとしてエクスポートするには、*【エクスポートするテキスト(Exported Text)】*フィールドでテキスト全体を選択し、CTRL+Cを押してコピーします。続いて、CTRL+Vを使用してすべての共通アプリケーション(テキストエディタなど)にこれを貼り付けます。
	ソート: 2つの矢印を使用してリストの各要素を上下に動かし、並べ替えることができます。

機能アイコン	意味
	PDF: 現在表示されているデータをPDFファイルに保存してから、保存したファイルをダウンロードするためのダイアログウィンドウが開きます。
	CSV: 現在表示されているデータをCSV(コンマ区切り値)ファイルに保存してから、保存したファイルをダウンロードするためのダイアログウィンドウが開きます。

2.6オブジェクトリスト

オブジェクトリストとは、WebAdminの左側に一時的に表示されるドラッグ&ドロップリストで、メインメニューをカバーします。

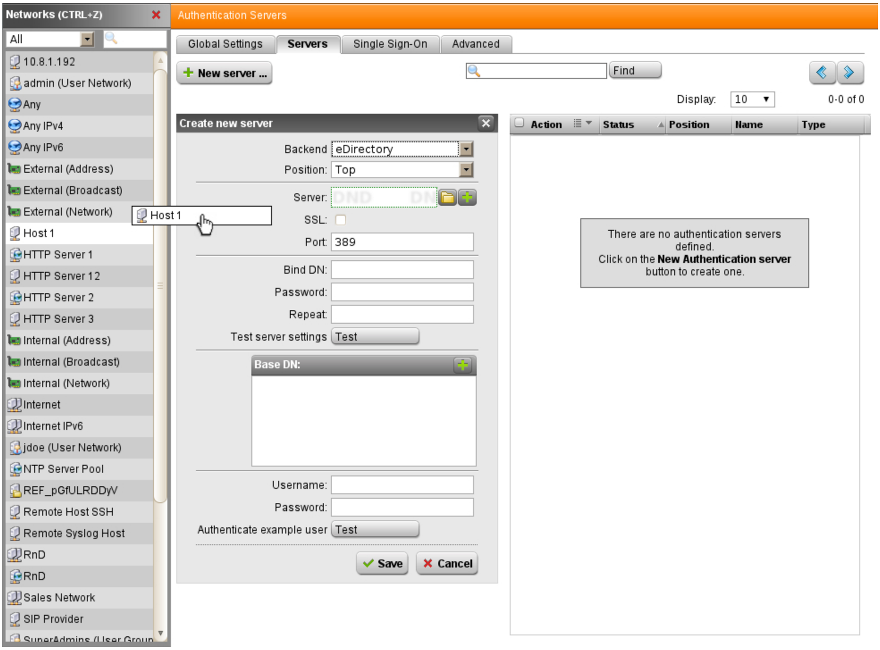


図8 WebAdmin:オブジェクトリストネットワークからのオブジェクトのドラッグ

オブジェクトリストは、フォルダアイコンをクリックすると自動的に開きます(上のセクションを参照)。あるいは、キーボードショートカットを使用して手動で開くこともできます(「マネジメン

*ト」>>「WebAdmin設定」>>「ユーザプリファレンス」*を参照)。
オブジェクトリストから、ユーザ/グループ、インタフェース、ネットワーク、サービスなどのWebAdminオブジェクトにすばやくアクセスし、設定時に選択することができます。オブジェクトを選択するには、現在の設定にオブジェクトをドラッグ＆ドロップするだけです。
既存の各種オブジェクトタイプに従い、オブジェクトリストには5つのタイプがあります。フォルダアイコンをクリックすると、現在の設定で必要なタイプが常に開きます。

３ダッシュボード

ダッシュボードは、Astaro Security Gatewayの現在の操作状況をグラフィカルに表示します。デフォルトで、ダッシュボードは5秒間隔で更新されます。更新間隔は【*無し(Never)*】～【*60秒(60 seconds)*】の間で設定できます。

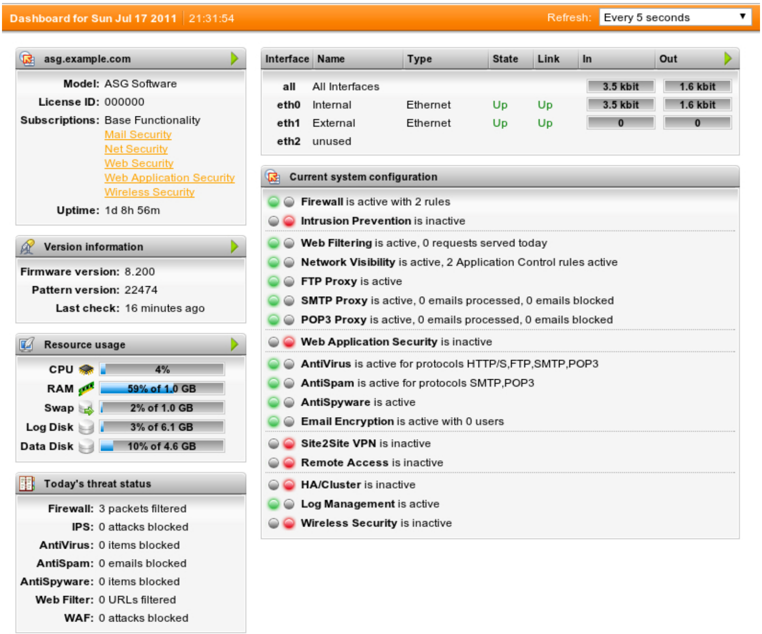


図9　WebAdmin：ASGソフトウェアのサンプルダッシュボード V8

このダッシュボードにはデフォルトで、ユーザがいつWebAdminにログインしたのかを示す情報と次の情報が表示されます。

- **一般情報(General Information)**：ユニット(装置)のホスト名、モデル、ライセンスID、アップタイム。
- **バージョン情報(Version Information)**：現在インストールされているファームウェアとパターンバージョン、および利用可能な更新パッケージの情報。
- **リソースの使用状況(Resource Usage)**：次のコンポーネントを含むシステムの現在の使用状況。

    - CPU使用率(%)
    - RAM使用率
    - スワップ使用率(%)
    - ログパーティションで消費されているハードディスクの容量(%)
    - ルートパーティションで消費されているハードディスクの容量(%)
    - UPS(無停電電源装置)モジュールがある場合はその状態
- **今日の脅威状況(Today's Threat Status)**: 深夜以降に検出された関連するセキュリティ脅威のカウンタ:
    - ログが有効になっているドロップされたデータパケットと拒否されたデータパケットの合計
    - 侵入がブロックされた回数の合計
    - ブロックされたウイルスの合計(全プロキシ)
    - ブロックされたスパムメッセージの合計(SMTP/POP3)
    - ブロックされたスパイウェアの合計(全プロキシ)
    - ブロックされたURLの合計(HTTP/S)
    - ブロックされたWebサーバ攻撃の合計(WAF)
- **インタフェース(Interfaces)**:設定されているネットワークインタフェースカードの名前とステータス。さらに、受信トラフィックと送信トラフィックの両方に対する過去75秒間の平均ビットレートに関する情報も表示されます。表示される値は、15秒間隔で収集されるサンプルに基づく平均ビットレートから取得されます。インタフェースのトラフィックアイコンをクリックすると、フローモニタが新しいウィンドウで開きます。フローモニタには、過去10分間のトラフィックが表示され、短い間隔で自動更新されます。フローモニタについて詳しくは、「フローモニタ」を参照してください。
- **現在のシステム設定(Current System Configuration)**: 関連セキュリティ機能が有効であるか無効であるかを示します。
    - **ファイアウォール(Firewall)**: アクティブファイアウォールルールの合計に関する情報。
    - **侵入防御(Intrusion Prevention)**: 侵入防御システム(IPS)は、シグニチャに基づくIPSルールセットを利用して攻撃を認識します。
    - **Webフィルタ(Web Filter)**:HTTP/Sプロトコル用のアプリケーションレベルのゲートウェイ。サービスの使用が許可されているネットワークに対し、豊富なWebフィルタ技術を提供します。

- **ネットワークの可視性(Network Visibility)**: Astaroのレイヤ7アプリケーションコントロールを使用すると、ネットワークトラフィックを分類およびコントロールできます。
- **FTPプロキシ(FTP Proxy)**: FTP*(ファイル転送プロトコル)*を使用したファイル転送用のアプリケーションレベルのゲートウェイ。
- **SMTPプロキシ(SMTP Proxy)**: SMTP*(簡易メール転送プロトコル)*を使用したメッセージ送信用のアプリケーションレベルのゲートウェイ。
- **POP3プロキシ(POP3 Proxy)**: POP3*(Post Office Protocol 3)*を使用したメッセージ送信用のアプリケーションレベルのゲートウェイ。
- **Webアプリケーションセキュリティ(Web Application Security)**: Webサーバをクロスサイトスクリプティングや SQLインジェクションなどの攻撃から防御するためのアプリケーションレベルのゲートウェイ。
- **アンチウイルス(AntiVirus)**: ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを伝送するWebトラフィックからネットワークを保護します。
- **アンチスパム(AntiSpam)**: 未承諾のスパムメールを検知し、既知の(または疑わしい)スパム発信者からのスパム送信を特定します。
- **アンチスパイウェア(AntiSpyware)**: シグニチャデータベースとスパイウェアフィルタリング技術が定期的に更新される2種類のウイルススキャンエンジンを使用して、スパイウェア感染を防止します。受信トラフィックと送信トラフィックの両方を保護します。
- **メール暗号化(E-mail Encryption)**: S/MIMEまたはOpenPGP標準によってEメールを暗号化、復号化、デジタル署名します。
- **サイト間VPN(Site2Site VPN)**: サイト間VPNシナリオの設定。
- **リモートアクセス(Remote Access)**: ロードウォリアVPNシナリオの設定。
- **HA/クラスタ(HA/Cluster)**: 冗長化(HA)フェイルオーバおよびクラスタリング。つまり、処理集約型のタスク(コンテンツフィルタ、ウイルススキャン、侵入検知、復号化など)を複数のクラスタノードに均一に分散します。
- **ログ管理(Log Management)**: ネットワーク内外のマシンからのログファイルを一括して保存します。ログは、定義したイベント時の自動通知を含め、簡単に検索およびモニタリングできます。
- **ワイヤレスセキュリティ(Wireless Security)**: ワイヤレスネットワークおよびアクセスポイントの設定。

3.1 フローモニタ

Astaro Security Gatewayのフローモニタは、現在ASGのインタフェースを通過しているネットワークトラフィックに関する情報を素早く確認するためのアプリケーションです。ダッシュボードの右上でいずれかのインタフェースをクリックすることにより簡単にアクセスできます。【*すべてのインタフェース(All Interfaces)*】をクリックすると、すべてのアクティブなインタフェースについて蓄積されたトラフィックがフローモニタに表示されます。単一のインタフェースをクリックすると、そのインタフェースのトラフィックのみがフローモニタに表示されます。

注 - フローモニタは新しいブラウザウィンドウで開きます。このウィンドウはポップアップブロッカによってブロックされる可能性があるため、WebAdminに対してポップアップブロッカを無効にすることをお勧めします。

フローモニタには、グラフとテーブルという2種類のビューがあります。それぞれについては後述します。ビューは5秒間隔で更新されます。更新を停止するには【*一時停止(Pause)*】ボタンをクリックします。【*続行(Continue)*】をクリックして更新を再開すると、フローモニタが最新のトラフィック情報に更新します。

グラフビュー

フローモニタのグラフには、過去10分間のネットワークトラフィックが表示されます。横軸は時間を、縦軸はスループットにスケールを動的に適用したときのトラフィック量を示します。

グラフビューの下部には、インタフェースを通過するトラフィックの種類を示す凡例が表示されます。トラフィックは種類ごとに色分けされるため、グラフ内で簡単に見分けることができます。

注 - ネットワークの可視性(Netowork Visibility)を有効にした場合(*「Webセキュリティ」>>「アプリケーションコントロール」>>「ネットワークの可視性」*の章を参照)、フローモニタはトラフィックについてより差別化された情報を表示します。

マウスのカーソルをグラフ上に置くと、大きなドット(点)が表示され、グラフのその部分の詳細な情報が表示されます。このドットは、グラフの線に沿って移動します。マウスのカーソルを移動すると、ドットもそれに従って移動します。グラフに何本かの線がある場合、ドットはマウスカーソルの移動に従って線の間を移動します。さらに、ドットの色は、それが表示している情報がどの線に関連するかによって変わるため、線が互いに近接している場合に役立ちます。ドットは、ある時点でのトラフィックの種類とサイズに関する情報を示します。

テーブルビュー

フローモニタのテーブルには、過去5秒間のネットワークトラフィックに関する情報が表示されます。

#: トラフィックは、現在の帯域幅使用状況に基づいてランク付けされます。

アプリケーション(Application): 利用可能な場合、ネットワークトラフィックのプロトコルまたは名前。未分類のトラフィックは、システムにとって不明な種類のトラフィックです。

クライアント(Clients): トラフィックに関与するクライアントの数。

現在の帯域幅使用状況(Bandwidth Usage Now): 過去5秒間の帯域幅使用状況。

合計トラフィック(Total Traffic): 接続の「ライフタイム」中に生成されたネットワークトラフィックの合計数。例1: ダウンロードが、過去のある時点で開始され、まだ継続中です。ダウンロード開始時点から、期間中に生成されたトラフィック全体が表示されます。例2: 複数のクライアントがFacebookを使用しています。いずれか1つのクライアントが接続をオープンにしている限り、すべてのクライアントによってこれまでに生成されたトラフィックがすべて蓄積されて合計トラフィックに表示されます。

アクション(Actions): アプリケーションの種類に応じて、利用可能なアクションがあります。

- ブロック(Blocking): 赤いブロックシンボルをクリックすると、現時点から該当アプリケーションがブロックされます。これにより、【*アプリケーションコントロールルール(Application Control Rules)*】ページにルールが作成されます。このオプションは、Astaro Security Gatewayの正常なオペレーションに必要なアプリケーションに対しては利用できません。たとえば、WebAdminトラフィックはブロックできません。これをブロックすると、ユーザ自身がWebAdminからシャットアウトされてしまいます。未分類のトラフィックもブロックできません。

- トラフィックシェーピング(Traffic shaping): オレンジとグレーのシェーピングシンボルをクリックすると、当該アプリケーションのトラフィックシェーピングが有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら【*保存(Save)*】をクリックします。これにより、【*トラフィックセレクタ(Traffic Selectors)*】ページにルールが作成されます。
  シェーピングはインタフェース単位で機能するため、【*すべてのインタフェース(All Interfaces)*】フローモニタを閲覧している際はトラフィックシェーピングを利用できません。

4マネジメント

この章では、基本システム設定や、Astaro Security Gateway、*WebAdmin*などのWebベース管理インタフェースの設定を定義する方法を説明します。【*概要(Overview)*】ページには、加えられた可能性のある変更を含め、最近のWebAdminセッションの統計が表示されます。変更の詳細を確認するには、【*変更ログ(Changelog)*】列の【*表示(Show)*】ボタンをクリックします。

この章には次のトピックが含まれます。

- システム設定
- WebAdmin設定
- ライセンス
- Up2Date
- バックアップ/リストア
- ユーザポータル
- 通知
- カスタマイズ
- SNMP
- 集中管理
- 冗長化
- シャットダウン/リスタート

4.1システム設定

【*システム設定(System Settings)*】の下にあるタブで、ホスト名、日付、時刻など、ゲートウェイ設定を行うことができます。

4.1.1組織

御社の名前と所在地、および当製品の運用を技術的に担当されるご担当者様または担当部署のEメールアドレスを入力します。Astaro Security Gateway.このデータは、IPsec、Eメール暗号化、およびWebAdminの証明書でも使用されます。

4.1.2ホスト名

このフィールドにゲートウェイホスト名を*完全修飾ドメイン名*(FQDN)で入力します(例:`ASG.example.com`)。ホスト名には英数字、ドット、およびハイフンを使用できます。ホスト名の末尾には`com`、`org`、`de`などの特殊な識別子を使用する必要があります。ホスト名は、通知メッセージでゲートウェイを識別するために使用されます。また、Web Webフィルタから送信されたステータスメッセージにも表示されます。お客様のドメインのDNSゾーンにホスト名を登録する必要はありません。

4.1.3日付と時刻

ゲートウェイでは、日付と時刻を常に正しく設定しておく必要があります。これは、ロギングおよびレポーティングシステムから正しい情報を取得したり、インターネット上の他のコンピュータとの相互運用性を保証するために必要です。

通常は、日付と時刻を手動で設定する必要はありません。デフォルトで、パブリックのインターネットサーバとの自動同期が有効化されています(*「インターネットサーバと時間を同期」*のセクションを参照)。

まれではありますが、タイムサーバとの同期を無効にする必要がある場合、時刻と日付を手動で変更することができます。ただし、これを行う場合は、以下の警告に注意してください。

- システム時間を標準時間からサマータイムに(あるいはその逆に)変更しないでください。この変更は、タイムサーバとの自動同期を無効にした場合でも、タイムゾーンの設定によって自動的に行われます。
- タイムサーバとの同期が有効になっている場合は、日付または時刻を手動で変更しないでください。多くの場合、自動同期により、手動で行った変更がすぐに取り消されます。日付または時刻を手動で設定する必要がある場合、最初に【*NTPサーバ(NTP Servers)*】ボックス(下の【*インターネットサーバと時間を同期(Synchronize Time With Internet Server)*】セクション)からすべてのサーバを削除し、【*適用(Apply)*】をクリックしてください。

- システム時間を手動で変更してから、変更が成功したことを通知する緑色の確認メッセージが表示されるまで待機します。次に、システムをリブートします(【マネジメント(Management)】>>【シャットダウン/リスタート(Shutdown/Restart)】)。多くのサービスでは、時間は連続的に変化し、急に変化する訳ではないという事実に依存しているため、これが推奨されます。時間に飛びがあると、様々なサービスの誤作動につながる可能性があります。このアドバイスは、あらゆる種類のコンピュータシステムに共通して該当します。
- まれに、システム時間を変更すると、WebAdminセッションが強制終了される可能性があります。これが発生した場合、ログインし直して、時刻が正しく設定されていることを確認し、後でシステムを再起動してください。

いくつかのタイムゾーンにまたがる相互接続された複数のゲートウェイを運用している場合は、すべてのデバイスに同じタイムゾーンを選択します(例:UTC(協定世界時))。これにより、ログメッセージをより簡単に比較できます。

システム時間を手動で変更すると、システムを正しく再起動した場合でも、複数の副作用が予想されます。

- **時刻を早める**
  - 時刻に基づくレポートの場合、スキップされた時間のデータがなくなります。ほとんどのグラフでは、この期間は、最近記録された値が直線で表示されます。
  - アカウンティングレポートでは、この期間は、すべての変数が0で表示されます。
- **時刻を戻す**
  - 時刻に基づくレポートには、該当する期間のログデータがすでに存在します。
  - ほとんどの図は、この期間に記録された値を圧縮して表示します。
  - ダッシュボードで表示される最後のパターンチェックからの経過時間は、たとえ最後のチェックがほんの数分前に行われた場合であっても、値について「なし」と表示します。
  - ASG上で自動的に作成された証明書は、それらの有効期間の開始日付が将来になっている場合は無効になります。
  - アカウンティングレポートは将来の時刻から記録された値を保持します。再度リセットの時刻になると、アカウンティングデータは再度通常どおりに記述されます。

こうした欠点があるため、システム時刻はシステムのセットアップ時に一度だけ設定し、その後は少し調整するだけにするべきです。これは、レポートデータをさらに処理する必要がある場合やデータの精度が重要な場合には、特に言えることです。

日付および時間を設定(Set Time And Date)

システム時刻を手動で設定するには、日付と時刻をそれぞれのドロップダウンリストから選択します。設定を保存するには【*適用(Apply)*】をクリックします。

タイムゾーンを設定(Set Timezone)

システムのタイムゾーンを変更するには、ドロップダウンリストから地域またはタイムゾーンを選択します。設定を保存するには【*適用(Apply)*】をクリックします。

インターネットサーバと時間を同期(Synchronize Time With Internet Server)

タイムゾーンを変更してもシステム時間は変更されず、影響があるのは、ロギングデータやレポーティングデータなどの出力における時間の表示のみです。したがって、サービスの妨げとなることはなく、後でシステムをリブートする必要はありません。ただし、時刻の変更と同様に、ロギングおよびレポーティングデータには影響があります。

タイムサーバを使用してシステム時刻の同期をとるには、1台以上のNTP サーバを選択します。設定を終了したら【*適用(Apply)*】をクリックします。

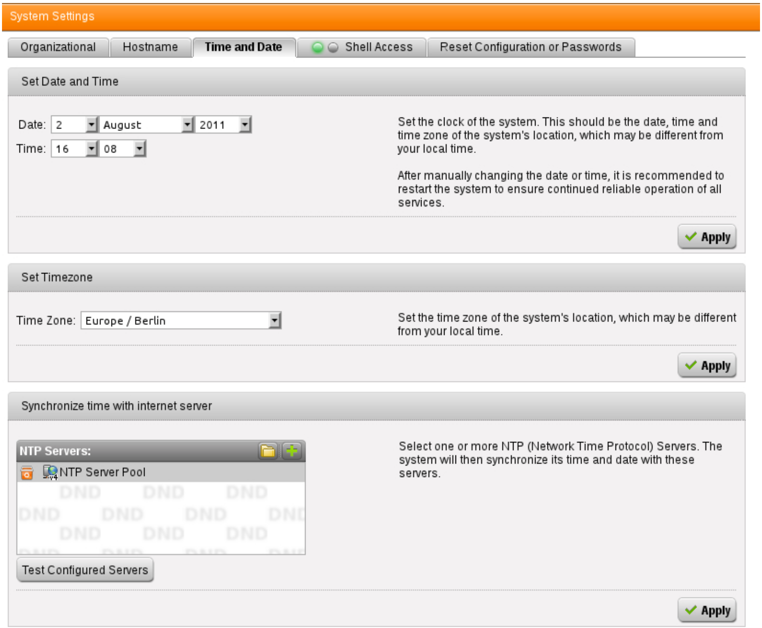


図10 システム設定：日付および時間を設定

NTPサーバ(NTP Servers)：デフォルトでは【*NTPサーバプール(NTP Server Pool)*】が選択されています。このネットワーク定義は*pool.ntp.org*プロジェクトのパブリックタイムサーバの大きな仮想クラスタにリンクしています。インターネットサービスプロバイダが顧客用にNTPサーバを運用しており、これらのサーバへのアクセス権がある場合、*NTPサーバプール*を削除してプロバイダのサーバを使用することが推奨されます。独自のサーバまたはプロバイダのサーバを選択する場合、複数のサーバを使用すると、精度や信頼性が向上します。3つの独立したサーバを使用すれば、常に十分です。それ以上のサーバを追加しても、さらなる改良はほとんど期待できず、サーバの負荷が増加します。*NTPサーバプール*と独自またはプロバイダのサーバの両方を使用しても、精度や信頼性は向上しないため、使用は推奨されません。

テスト構成サーバ(Test Configured Servers)：デバイスから選択されたNTPサーバへの接続を確立できることと、NTPサーバが使用可能な時刻データを返すことをテストする際は、このボタンをクリックします。これで、お使いのシステムとサーバ間の時間のオフセットを測定します。お使いのシステムが正しく設定されており、一定時間にわたって安定した状態で動作している場合は、オフセットは一般的に1秒未満になります。

通常、NTPを有効化したり他のサーバを追加した直後は、オフセットがこれより長くなります。時間の飛びを防ぐために、NTPはゆっくりとシステム時間をずらします。やがて、システム時間は時間

の飛びなく補正されます。このような状況が発生した場合は、しばらく待機してください。特に、このような場合には、システムを再起動しないでください。その代わりに、約1時間後に再びチェックしてください。オフセットが減少すると、すべてが正しく機能するようになります。

4.1.4シェルアクセス

セキュアシェル(SSH)はコマンドラインアクセスモードであり、主にゲートウェイへのリモートシェルアクセスを取得するために使用されます。これは通常、低レベルのメンテナンスやトラブルシューティングに使用されます。このシェルにアクセスするには、SSHクライアントが必要です。SSHクライアントは一般的に、ほとんどのLinuxディストリビューションに装備されています。

許可ネットワーク(Allowed Networks)

【*許可ネットワーク(Allowed Networks)*】コントロールを使用して、この機能へのアクセスを特定ネットワークのみに制限します。ここにリストされたネットワークは、SSHサービスに接続できます。

認証(Authentication)

このセクションで、SSH アクセスの認証方法とアクセスの厳格さを定義できます。以下の認証方法を利用できます。

- パスワード(デフォルト)
- 公開鍵
- パスワードと公開鍵

【*公開鍵認証(Public Key Authentication)*】を使用するには、公開鍵での認証を許可された各ユーザーについて、それぞれの公開鍵を【*ログインユーザに承認された鍵(Authorized Keys For Loginuser)*】フィールドにアップロードする必要があります。

ルートログインの許可(Allow Root Login): ルートユーザに対してSSHアクセスを許可できます。このオプションを有効にするとセキュリティリスクが高くなるため、デフォルトでは無効になっています。このオプションを有効にすると、ルートユーザは公開鍵を介してログインできます。【*ルートに承認された鍵(Authorized Keys For Root)*】フィールドにルートユーザの公開鍵をアップロードします。

設定を保存するには【*適用(Apply)*】をクリックします。

シェルユーザパスワード(Shell User Passwords)

デフォルトのシェルアカウント`root`(ルート)および`loginuser`(ログインユーザ)用のパスワードを入力します。これら2つのアカウントのいずれか一方のパスワードのみを変更するには、他方のアカウントの入力ボックスを空白のままにします。

注 - SSHシェルアクセスを有効にするには、最初にパスワードを設定する必要があります。さらに、【*定義およびユーザ(Definitions & Users)*】>>【*認証サーバ(Authentication Servers)*】>>【*詳細(Advanced)*】タブで設定したパスワードの複雑さの設定に準拠したパスワードのみを指定できます。つまり、複雑なパスワードを有効にした場合は、シェルユーザのパスワードも同じ要件を満たすことが必要になります。

SSHデーモンリスンポート(SSH Daemon Listen Port)

このオプションで、SSHに使用するTCPポートを変更できます。デフォルトでは、標準SSHポートの`22`が設定されています。ポートを変更するには、`1024`～`65535`の適切な値を【*ポート番号(Port Number)*】ボックスに入力し、【*適用(Apply)*】をクリックします。

4.1.5設定またはパスワードのリセット

【*設定またはパスワードのリセット(Reset configuration or passwords)*】タブのオプションで、シェルユーザのパスワードを削除できます。さらに、工場出荷時の状態に戻すことができます。

システムパスワードのリセット(Reset System Passwords): この機能を実行すると、以下のユーザのパスワードがリセットされます。

- ルートユーザ(シェルユーザ)
- ログインユーザ(シェルユーザ)
- admin(事前に定義されている管理者アカウント)

さらに、システムを停止するには、【*後でシステムをシャットダウン(Shutdown System Afterwards)*】オプションを選択します。

セキュリティに関する注記 - 次にWebAdminに接続する人に対して、【*adminパスワード設定(Admin Password Setup)*】ダイアログウインドウが表示されます。したがって、パスワードをリセットしたら、すぐにログアウトし、ブラウザでそのページをリロード(再読み込み)して、新しいadminパスワードを設定してください。

また、【*マネジメント(Management)*】>>【*システム設定(System Settings)*】>>【*シェルアクセス(Shell Access)*】タブで新しいシェルパスワードを設定しない限り、シェルアクセスは実行できなくなります。

工場リセット(Factory Reset):この機能は、工場出荷時のデフォルトの設定にデバイスをリセットします。以下のデータが削除されます。

- システム設定
- Webフィルタキャッシュ
- ログおよびレポーティングデータ
- データベース
- 更新パッケージ
- ライセンス
- パスワード
- 高可用性ステータス

ただし、Astaro Security Gateway ソフトウェアのバージョン番号はそのままです。つまり、インストールされたすべてのファームウェアおよびパターンの更新が維持されるということです。

注 -Astaro Security Gateway は、工場リセットが開始するとシャットダウンします。

4.2WebAdmin設定

*【マネジメント(Management)】>>【WebAdmin設定(WebAdmin Settings)】*の下にあるタブで、TCPポート、ユーザ設定、およびWebAdminの言語といったWebAdminの基本設定を構成できます。

4.2.1一般

*【WebAdmin設定(WebAdmin Settings)】>>【一般(General)】*タブで、WebAdmin言語と基本アクセス設定を構成できます。

WebAdmin言語(WebAdmin Language)

WebAdminの言語を選択します。これは現在のユーザプロファイルのみに適用されます。

WebAdminアクセス設定(WebAdmin Access Configuration)

ここで、WebAdminへのアクセスが許可されるユーザやネットワークを設定できます。

許可された管理者(Allowed Administrators):Astaro Security Gateway は同時に複数の管理者によって管理できます。*【許可された管理者(Allowed Administrators)】*ボックスで、WebAdminインタフェースへの無制限の読み取りおよび書き込みアクセスを持つユーザまたはグループを指定できます。デフォルトでは、これは*SuperAdmins*のグループになります。

許可ネットワーク(Allowed Networks):*【許可ネットワーク(Allowed Networks)】*ボックスで、WebAdminインタフェースに接続できるネットワークを定義できます。ゲートウェイをスムーズにインストールするために、デフォルトは【すべて(Any)】になっています。これは、WebAdminインタフェースはどこからでもアクセスできることを意味します。この設定は、できるだけ早く内部ネットワークに変更してください。ただし、最もセキュアなソリューションは、ゲートウェイへのアクセスを、HTTPS経由の1台の管理者用PCのみに制限することです。

アクセストラフィックをログ(Log Access Traffic): すべてのWebAdminアクセスアクティビティをファイアウォールログにログする場合は、*【アクセストラッフィックをログ(Log Access Traffic)】*チェックボックスにチェックを入れます。

4.2.2アクセスコントロール

【WebAdmin設定(WebAdmin Settings)】>>*【アクセスコントロール(Access Control)】*タブで、特定のユーザに対してWebAdmin役割を作成することができます。これにより、WebAdminユーザに付与できる権限を細かく定義することができます。

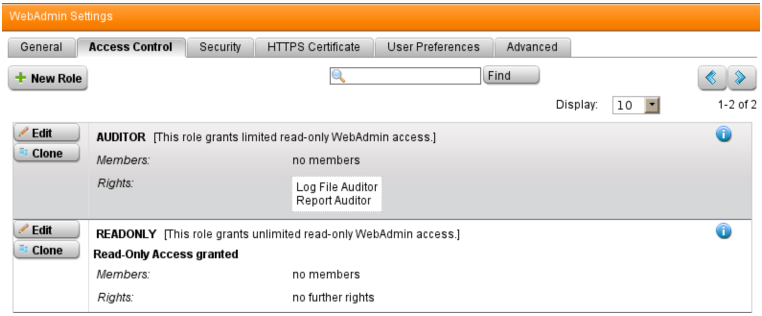


図11 WebAdmin設定:アクセスコントロールの設定

以下の2つのユーザ役割があらかじめ定義されています。

監査担当者(Auditor): この役割のユーザは、ログデータやレポートデータを参照できます。

読取専用(Readonly): この役割のユーザは、WebAdmin内のすべてを参照できますが、編集、作成、削除は一切できません。

これらのいずれかの役割をユーザまたはグループに割り当てるには、*【編集(Edit)】*ボタンをクリックし、各ユーザまたはグループを*【メンバ(Members)】*ボックスに追加します。

セキュリティポリシに応じて、追加の役割を作成することができます。以下の手順に従ってください。

1. **【アクセスコントロール(Access Control)】タブで、【新規役割(New Role)】をクリックします。**
   *【役割の作成(Create Role)】*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name): この定義を説明する名前を入力します。

   メンバ(Members): この役割を割り当てるユーザとグループをこのボックスに追加します。

   読取専用アクセスを付与(Grant Read-Only Access)(オプション): このチェックボックスにチェックを入れると、WebAdminのすべてのエリアへの読取専用アクセスが、指定メンバに付与されます。

   権限(Rights): このボックスでは、WebAdminの異なる職種(監査担当者とマネージャ)に対し、異なる権限レベルが含まれています。マネージャは各機能に対する完全な管理権限を持ちますが、監査担当者は参照権限のみです。権限の前にあるチェックボックスにチェックを入れて、1つ以上の権限を選択することができます。
   例: ユーザJon Doeに、メールセキュリティのマネージャ権限を付与し、追加で*【読取専用アクセスを付与(Grant Read-Only Access)】*チェックボックスにチェックを入れるとします。このユーザは、メールセキュリティのセクションでは設定を変更できますが、WebAdminのその他のエリアでは参照のみ可能で、変更は一切できません。

   コメント(Comment)(オプション): 説明などの情報を追加します。
3. **【保存(Save)】をクリックします。**
   設定が保存されます。

役割を編集または削除するには、対応するボタンをクリックします。*監査担当者*と*読取専用*の各役割は削除できません。

4.2.3セキュリティ

パスワード推測をブロック(Block Password Guessing): この機能を使用してパスワードが推測されないようにします。設定した回数のログインに失敗すると(デフォルトでは3回)、WebAdminアクセスを取得しようとしているIPアドレスは設定した時間(デフォルトでは600秒間)ブロックされます。*【ブロック対象外ネットワーク(Never Block Networks)】*ボックスにリストされているネットワークは、このチェックから除外されます。

4.2.4HTTPS証明書

*【マネジメント(Management)】>>【WebAdmin設定(WebAdmin Settings)】>>【HTTPS証明書(HTTPS Certificate)】*タブで、WebAdmin CA証明書をブラウザにインポートしたり、WebAdmin証明書を再生成したり、WebAdminとユーザポータルでの署名証明書の使用を選択したりできます。

WebAdminアクセスの初回セットアップ時に、ローカルCA証明書をゲートウェイで作成しました。このCA証明書の公開鍵をお使いのブラウザにインストールすると、WebAdminインタフェースへのアクセス時にセキュリティ警告が表示されなくなります。

> **注 -**Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの*【インターネットオプション】*>>*【セキュリティ】*で設定します。さらに、Internet Explorer 7を使用する場合は、*【信頼済みサイトゾーン】*で*【ファイルのダウンロード時に自動的にダイアログを表示】*を選択します。

CA証明書をインポートするには、以下の手順に従います。

1. ***【HTTPS証明書(HTTPS Certificate)】*タブで、*【CA証明書をインポート(Import CA Certificate)】*をクリックします。**
   CA証明書の公開鍵がエクスポートされます。

   CA証明書の公開鍵は、ディスクに保存するか、お使いのブラウザにインストールできます。

2. **証明書をインストールします**(オプション)。
   ブラウザにダイアログボックスが表示され、証明書のインストールをすぐに選択できます。

> **注 -** システム時刻とタイムゾーンの違いによって証明書を作成してもすぐに有効にならない場合があります。この場合、ほとんどのブラウザでは、証明書が期限切れであると表示されますが、この表示は間違っています。ただし、証明書は24時間以内には自動的に有効になり、その後27年間有効期間が持続します。

WebAdmin証明書の再生成(Re-generate WebAdmin Certificate)

WebAdmin証明書は、お客様が初回ログイン時に指定したホスト名を参照します。その間にホスト名が変更された場合は、ブラウザがセキュリティ警告を表示します。この問題を避けるために、新しいホスト名を考慮に入れて証明書を作成できます。このようなホスト名を入力して*【適用(Apply)】*をクリックします。証明書の変更後、WebAdminで引き続き作業を行うには、多く

の場合、お使いのWebブラウザでページをリロード(再読み込み)し、新しい証明書を承認して、Webadminに再度ログインする必要があります。

WebAdmin/ユーザポータル証明書の選択(Choose WebAdmin/User Portal Certificate)

CA証明書をインポートする代わりに、独自に署名した証明書をWebAdminおよびユーザポータルで使用したい場合、ここでその証明書を選択します。ただし、ドロップダウンリストで証明書を選択できるようにするためには、最初に*【リモートアクセス(Remote Access)】>>【証明書管理(Certificate Management)】>>【証明書(Certificates)】*タブにおいて、証明書、CA、秘密鍵が含まれる証明書をPKCS#12形式でアップロードする必要があります。アップロードされた証明書を使用するには、*【証明書(Certificates)】*ドロップダウンリストから選択し、*【適用(Apply)】*をクリックします。

4.2.5ユーザ設定

*【マネジメント(Management)】>>【WebAdmin設定(WebAdmin Settings)】>>【ユーザ設定(User Preference)】*タブで、現在ログインしているユーザのためにグローバルショートカットやページあたりのアイテムといったユーザプリファレンス(基本設定)を構成できます。

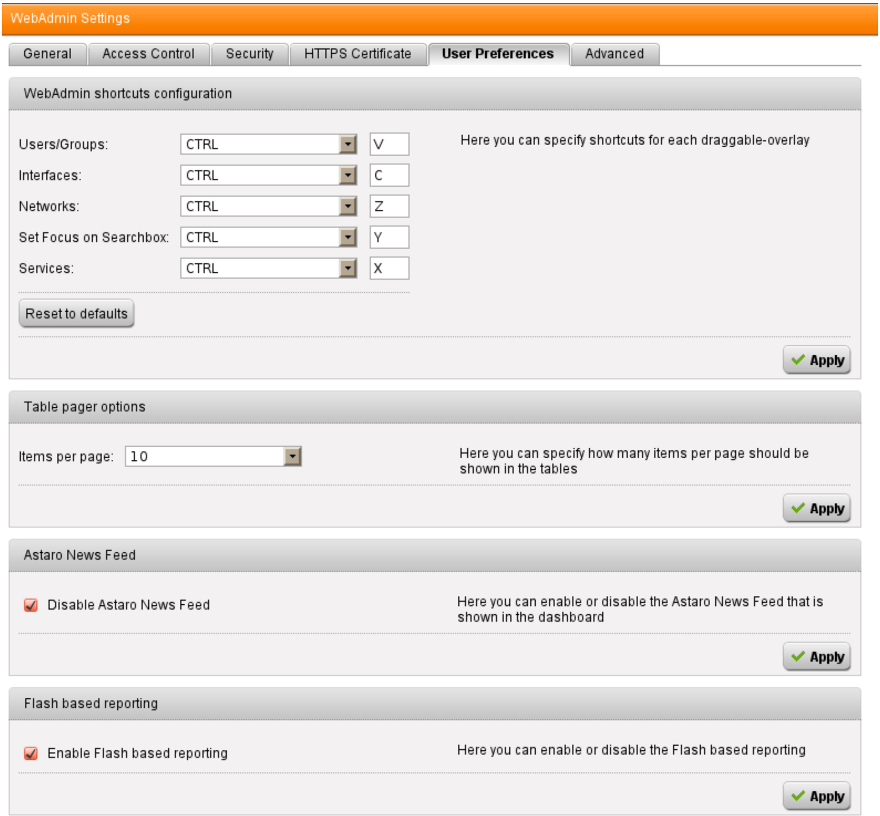


図12　WebAdmin設定：ユーザ設定の内容

WebAdminショートカットの設定

ここでは、多くの設定に使用されるドラッグ＆ドロップのオブジェクトリストを開いたり閉じたりするためのキーボードショートカットを設定できます（詳細は、「*WebAdmin*」>>「*オブジェクトリスト*」を参照）。また、検索ボックスのカーソルフォーカスを設定できます（「*WebAdmin*」>>「*WebAdminメニュー*」を参照）。ドロップダウンリストを使用して、Alt、Ctrl、Shiftなどの各種修飾キーとテキストボックスを選択し、異なる文字を入力してください。また、ドロップダウンリストで【*オフ（Off）*】を選択して、キーボードショートカットをオフにできます。

デフォルトの設定に戻るには、【*デフォルトにリセット（Reset to Defaults）*】ボタンをクリックします。設定を保存するには【*適用（Apply）*】をクリックします。

テーブルページャオプション(Table Pager Options)

ここでWebAdminのテーブルのページネーション(ページ割り)、つまり、ページあたりのアイテムの表示数をグローバルに定義できます。ドロップダウンリストをクリックして値を選択します。設定を保存するには【*適用(Apply)*】をクリックします。

Astaroニュースフィード(Astaro News Feed)

Astaroニュースフィードを有効にすると、ダッシュボード上の小さなセクションでAstaroやAstaro製品に関するニュースが提供されます。これはデフォルトでは無効になっています。ニュースフィードを有効にするには、【*Astaroニュースフィードを無効にする(Disable Astaro News Feed)*】チェックボックスのチェックを外します。設定を保存するには【*適用(Apply)*】をクリックします。

Flashベースのレポーティング

Astaro Security Gatewayのレポーティングセクションのグラフは、デフォルトでAdobe® Flash®アニメーションとして表示されます。これらのレポーティンググラフを表示するには、お使いのブラウザにFlash Playerプラグインをインストールする必要があります。Flash PlayerプラグインをインストールしていないかFlashを使用したくない場合は、【*Flashベースのレポーティングを有効にする(Enable Flash-based Reporting)*】チェックボックスのチェックを外してFlashベースのレポーティングを無効にしてください。無効にすると、グラフは静止画像で表示されるようになります。*ただし*、Flashベースのレポーティングを無効にすると、一部のレポーティング表示機能が失われます。設定を保存するには【*適用(Apply)*】をクリックします。

4.2.6詳細

WebAdminアイドルタイムアウト(WebAdmin Idle Timeout)

待ち時間(Log Out After): このフィールドでは、どれぐらいWebAdminセッションのアイドル期間が続いたら管理者に再度ログインを要求するかを秒単位で指定できます。デフォルトでは、アイドルタイムアウトは300秒に設定されています。指定できる範囲は60～86,400秒です。

ダッシュボードでログアウト(Log Out on Dashboard):デフォルトで、WebAdminの【ダッシュボード(Dashboard)】ページ*を開くと、自動ログアウト機能は無効になっています。ただし*、このオプションを選択して、自動ログアウト機能をダッシュボードでも有効化することができます。

WebAdmin TCPポート(WebAdmin TCP Port)

デフォルトでは、ポート`4444`をWebAdminのTCPポートとして使用します。【*TCPポート(TCP Port)*】ボックスには、`443`あるいは`1024`～`65535`の任意の値を入力できます。*ただし*、一部のポートは他のサービス用に予約されています。特に、ポート`10443`は使用できません。また、ユーザポータルあるいはSSLリモートアクセスに使用しているものと同じポートは使用できません。

WebAdminにアクセスするときは、ブラウザのアドレスバーでポート番号をIPアドレスに(コロンで区切って)追加する必要があります。たとえば、`https://192.168.`のように指定します。

利用条件(Terms of Use)

会社ポリシで、WebAdminへのアクセスを求めるユーザに利用条件への同意を求めることができます。ユーザがWebAdminにログインするたびに利用条件に同意することを要求するには、【*ログイン後に「利用条件」を表示(Display "Terms of Use" After Login)*】チェックボックスにチェックを入れます。これにより、ユーザがログインすると利用条件が表示されるようになります。利用条件に同意しないと、再びログアウトされます。

必要に応じて利用条件の文面を変更することができます。設定を保存するには【*適用(Apply)*】をクリックします。

4.3ライセンス

Astaro Security Gatewayの特定の機能を使用できるか否かは、ライセンスとサブスクリプションによって定義されています。つまり、ゲートウェイとともに購入したライセンスとサブスクリプションに応じて、使用できる機能とできない機能があります。

2009年10月、Astaroは*オンデマンドライセンス*という新しいライセンスモデルを導入し、*従来のライセンス*から段階的に移行を進めています。お客様が購入された従来のライセンスも引き続き有効となります。

4.3.1ライセンスの取得方法

Astaroライセンスの購入後に、アクティベーションキーがEメールで送信されます。これらのキーを使用して、ライセンスを作成するか、既存のライセンスをアップグレードしてください。ライセンスを有効にするには、MyAstaroポータルにログインし、ライセンス管理のページにアクセスしてください。ページ上部にあるフォームの該当フィールドに、Eメールからアクティベーションキーをカット＆ペーストします。

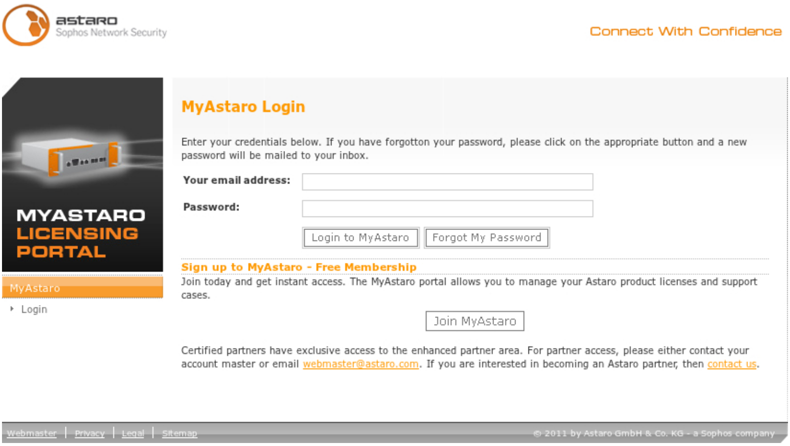


図13 MyAstaroポータル

別のフォームが表示されます。ここで、お客様がライセンスを購入した代理店についての情報と、お客様自身の詳細情報を入力してください。このフォームには、わかる限りの情報があらかじめ入力されています。また、該当する場合、AstaroはASG ハードウェアのシリアル番号をこのフォームから収集します。フォームの送信後、ライセンスが作成され、ライセンス詳細ページが表示されます。ここで、ライセンスファイルをダウンロードすることができます。

ライセンスを実際に使用する場合、ライセンスファイルをハードドライブにダウンロードして、インストールされているWebAdminにログインする必要があります。WebAdminで、*【マネジメント(Management)】>>【ライセンス(Licensing)】>>【インストレーション(Installation)】*タブにアクセスし、アップロード機能を使用してハードドライブ上のライセンステキストファイルを検索します。ライセンスファイルをアップロードすると、WebAdminがこれを処理して、すべてのサブスクリプションと、ライセンスに規定されたその他の設定を有効化します。

注 - Eメールで受信したアクティベーションキーをWebAdminにインポートすることはできません。このキーは、ライセンスの有効化だけに使用されます。ASGにインポートできるのはライセンスファイルのみです。

4.3.2オンデマンドライセンス

Astaroのオンデマンドライセンスモデルは、従来のライセンスモデルと比べてより簡単で柔軟性があります。まず、クラシックライセンスモデルの無料ホームユーザライセンスと似ている基本ライセン

スがあります。これは、基本機能を無料で提供するもので、すべてのホームユーザだけではなく、ビジネスユーザにもご利用いただけます。次に、3種類の購入サブスクリプションがあります。

- ネットセキュリティ
- Webセキュリティ
- メールセキュリティ

これらは、個別に購入することも組み合わせて購入することもできます。それぞれのサブスクリプションを使用して、製品の特定の機能を利用できます。下の表は、どのサブスクリプションでどの機能を使用できるかを示しています。

機能	**基本ライセンス**	**ネット**	**Web**	**メール**	**WAS**	**WS**
管理(バックアップ、通知、SNMP、ACCなど)	✓					
ローカル認証(ユーザ、グループ)	✓					
基本ネットワーキング(スタティックルーティング、DHCP、DNS、Auto QoS、NTPなど)	✓					
ファイアウォール/NAT(DNAT、SNATなど)	✓					
PPTP & L2TPリモートアクセス	✓					
ローカルログ、標準エグゼクティブレポート	✓					
侵入防御(パターン、DoS、フラッド、ポートスキャンなど)		✓				
IPsec & SSLサイト間VPN、IPsec & SSLリモートアクセス		✓				

機能	基本ライセンス	ネット	Web	メール	WAS	WS
アドバンストネットワーキング(リンクアグリゲーション、リンクバランシング、ポリシルーティング、OSPF、マルチキャスト、カスタムQoS、サーバ負荷分散、ジェネリックプロキシなど)		✔	(✔)	(✔)		
ユーザポータル		✔	✔	✔		
冗長化		✔	✔	✔		
リモート認証(AD、eDir、RADIUSなど)		✔	✔	✔		
リモートログ、詳細エグゼクティブレポート(アーカイブ、設定)		✔	✔	✔		
基本HTTP/S & FTPプロキシ			✔			
Web & FTPマルウェアフィルタリング			✔			
基本SMTPプロキシ、隔離レポート、メールマネージャ				✔		
SMTP & POP3マルウェアフィルタリング				✔		
Webアプリケーションセキュリティ					✔	
ワイヤレスセキュリティ						✔

サブスクリプションとその機能セットについて詳しくは、認定AstaroパートナーまたはAstaroホームページまでお問い合わせください。

Up2Date

各サブスクリプションは、自動更新を完全にサポートします。つまり、新しいファームウェアの更新に関する情報が自動的に通知されます。また、ファームウェアとパターン更新を自動的にダウン

ロード(およびインストール)できます。

サブスクリプションなしの基本ライセンスでは、自動更新に制限があります。オンラインヘルプの更新などのパターン更新に限り、自動的にダウンロードされ、インストールされますが、使用可能なファームウェア更新については通知されず、ファームウェア更新は手動でダウンロードする必要があります。新しいファームウェア更新については、Astaro Up2Dateブログで告知されます。

サポートとメンテナンス

基本ライセンスには*Webサポート*が含まれます。AstaroサポートフォーラムとAstaroナレッジベースをご利用いただけます。

サブスクリプションのうちいずれかを購入すると、お客様のサポート内容は自動的に*標準サポート*にアップグレードされ、MyAstaroポータルでサポートケースを開くことや、認定Astaroパートナーへの問い合わせが可能になります。

Astaroエンジニアが担当者となる24時間年中無休のサポートを提供する*プレミアムサポート*サブスクリプションを購入することもできます。

4.3.3クラシックライセンス

クラシックライセンスモデルは、上述のオンデマンドライセンスモデルに移行されます。クラシックライセンスはただちに無効になるわけではなく、段階的に移行が進められます。そのため、ここでは、互換性を維持するために従来のライセンスについて説明します。

Astaro Security Gateway には、すべての機能が有効になる30日間のトライアルライセンスが付属しています。このライセンスの期限満了後にAstaro Security Gatewayを操作したい場合には、有効なライセンスをインストールする必要があります。すべてのライセンス(無料のホームユーザライセンスを含む)はMyAstaroポータルで作成されます。

サブスクリプション

AstaroのWebフィルタリング機能(オプションのAstaro Security Gateway用サブスクリプションパッケージで提供)は、HTTP/S用にコンテンツフィルタリング、アンチウイルス、スパイウェア保護を、FTP用にアンチウイルス機能、ファイル拡張子スキャニングを提供します。

Webフィリタリングサブスクリプションが使用可能ではない場合、WebAdminの次のタブが無効になります。

- *【Webセキュリティ(Web Security)】>>【HTTP/S】>>【アンチウイルス/マルウェア(AntiVirus/Malware)】*

- *【Webセキュリティ(Web Security)】>>【HTTP/S】>>【URLフィルタリング(URL Filtering)】*
- *【Webセキュリティ(Web Security)】>>【HTTP/S】>>【URLフィルタリングカテゴリ(URL Filtering Categories)】*
- *【Webセキュリティ(Web Security)】>>【HTTP/Sプロファイル(HTTP/S Profiles)】>>【フィルタアクション(Filter Actions)】*
- *【Webセキュリティ(Web Security)】>>【FTP】>>【アンチウイルス(AntiVirus)】*

Astaroのメールセキュリティ機能は、Astaro Security Gatewayソリューションの2つの異なるサブスクリプションであるメールフィルタリング(Mail Filtering)とメール暗号化(Mail Encryption)によって提供されています。メールフィルタリングは、アンチスパム、アンチウイルス、フィッシング保護を提供します。一方、メール暗号化は、OpenPGPおよびS/MIME暗号化とSMTP Eメール用のデジタル署名を提供します。

メールフィリタリングサブスクリプションが使用可能ではない場合、WebAdminの次のタブが無効になります。

- *【メールセキュリティ(Mail Security)】>>【SMTP】>>【アンチウイルス(AntiVirus)】*
- *【メールセキュリティ(Mail Security)】>>【SMTP】>>【アンチスパム(AntiSpam)】*
- *【メールセキュリティ(Mail Security)】>>【POP3】>>【アンチウイルス(AntiVirus)】*
- *【メールセキュリティ(Mail Security)】>>【POP3】>>【アンチスパム(AntiSpam)】*
- *【メールセキュリティ(Mail Security)】>>【暗号化(Encryption)】*メニューのすべてのタブ

注 - 過去にメールフィルタリングまたはメール暗号化のいずれかのサブスクリプションを購入したことがあるお客様は、サブスクリプションのマージによるメリットを活用できます。これにより、両サブスクリプションの機能を使用できるようになります。

さらに、次の機能が無効になります。

- *【メールセキュリティ(Mail Security)】>>【SMTP】>>【リレー(Relaying)】>>【コンテンツスキャン(Content Scan)】*
- *【メールセキュリティ(Mail Security)】>>【SMTP】>>【詳細(Advanced)】>>【BATVシークレット(BATV Secret)】*
- *【メールセキュリティ(Mail Security)】>>【SMTP】>>【詳細(Advanced)】>>【最大メッセージサイズ(Max Message Size)】*
- *【メールセキュリティ(Mail Security)】>>【SMTPプロファイル(SMTP Profiles)】*

現在のライセンスがサブスクリプション機能をカバーしないことを示すために、タブの上に警告メッセージが表示されます。

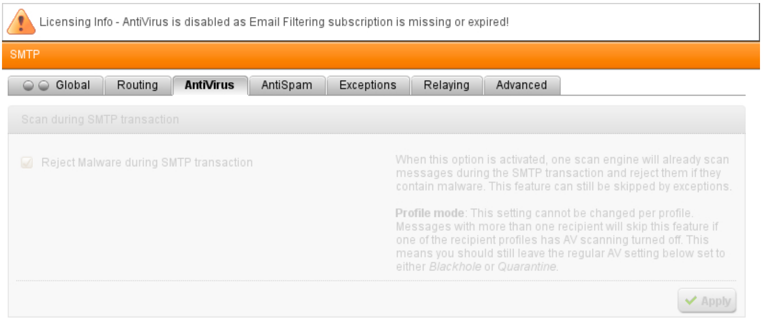


図14 ライセンス(Licensing):サブスクリプション警告メッセージ

4.3.4概要

【概要(Overview)】タブには、ライセンスに関する詳細情報が表示され、次のように複数のエリアに分割されています。

- **基本ライセンス(Base License)**:所有者、ID、有効期限などの基本的なライセンスパラメータが表示されます。
- **ネットワークセキュリティ、メールセキュリティ、Webセキュリティ、Webアプリケーションセキュリティ、ワイヤレスセキュリティ(Network Security, Mail Security, Web Security, Web Application Security, Wireless Security)**:サブスクリプションに関する情報(購入したものか否か、有効化されているか、有効期限、および提供する機能の簡単な説明など)が表示されます。
- **サポートサービス(Support Services)**:サポートレベルと有効期限が表示されます。

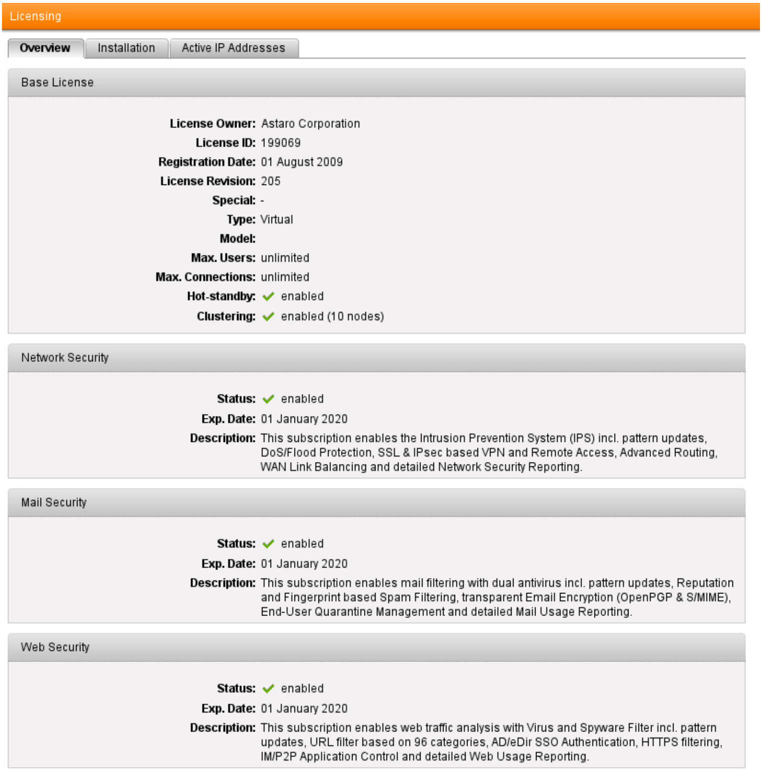


図15 ライセンス(Licensing):概要(オンデマンドライセンス)(Overview(OnDemand Licensing))

4.3.5インストール

*【マネジメント(Management)】>>【ライセンス(Licensing)】>>【インストール(Installation)】*タブでは、新しいライセンスのアップロードおよびインストールを実行できます。

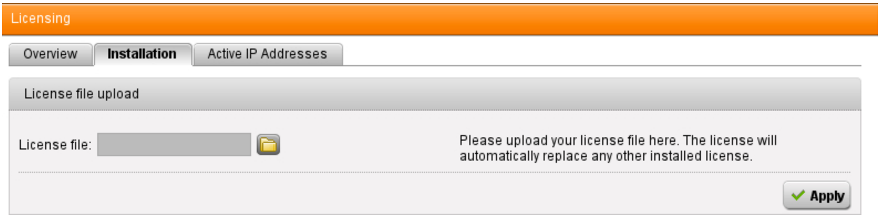


図16　ライセンス(Licensing):ライセンスのインストール

ライセンスをインストールするには、次の手順に従ってください。

1. ***【ファイルのアップロード(Upload File)】ダイアログボックスを開きます。***
   *【ライセンスファイル(License File)】*ボックスの横にあるフォルダアイコンをクリックします。

   *【ファイルのアップロード(Upload File)】*ダイアログボックスが開きます。

2. **ライセンスファイルを選択します。**
   ライセンスファイルが保存されているディレクトリを参照します。

   アップロードするライセンスファイルを選択します。

3. ***【保存(Save)】*をクリックします。**
   ライセンスファイルがアップロードされます。

4. ***【適用(Apply)】*をクリックします。**
   ライセンスがインストールされます。新しいライセンスは、すでにインストールされている他のライセンスを自動的に置き換えます。

   ライセンスのインストールには約60秒かかります。

4.3.6アクティブなIPアドレス

ユーザ(IPアドレス)が無制限に許可されるライセンスをお持ちでない場合は、お客様のライセンスでカバーされるIPアドレスに関する情報がこのタブに表示されます。お客様のライセンスの範囲外となるIPアドレスは、別のリストに記載されています。制限を超えると、定期的にEメール通知が送信されます。

注 - 7日間にわたって使用されなかったIPアドレスは、ライセンスカウンタから自動的に削除されます。

4.4Up2Date

*【マネジメント(Management)】>>【Up2Date】*メニューを使用して、Astaro Security Gatewayの更新サービスを設定できます。定期的に更新パッケージをインストールすることで、ゲートウェイを最新のバグフィックス、製品改善機能、およびウイルスパターンで保つことができます。各更新パッケージは、Astaroによってデジタル署名されています。署名がないものや偽造された更新は拒否されます。

2種類の更新を利用できます。

- **ファームウェアの更新**: ファームウェアの更新には、Astaro Security Gateway ソフトウェアのバグフィックスおよび拡張機能が含まれています。
- **パターンの更新**: パターンの更新によって、アンチウイルス、アンチスパム、侵入防止の定義、およびオンラインヘルプが最新状態に保たれます。

Up2Dateパッケージをダウンロードするために、ゲートウェイは更新サーバに対するTCP接続をポート`443`で開きます。このため、この接続は管理者の調整なしで使用できます。ただし、途中に別のファイアウォールがある場合は、ポート`443` TCPを介した更新サーバへの通信を明示的に許可する必要があります。

4.4.1概要

*【マネジメント(Management)】>>【Up2Date】>>【概要(Overview)】*タブには、お使いのシステムが最新のものであるかどうかを示す概要が表示されます。ここで、新しいファームウェアやパターンの更新パッケージをインストールできます。

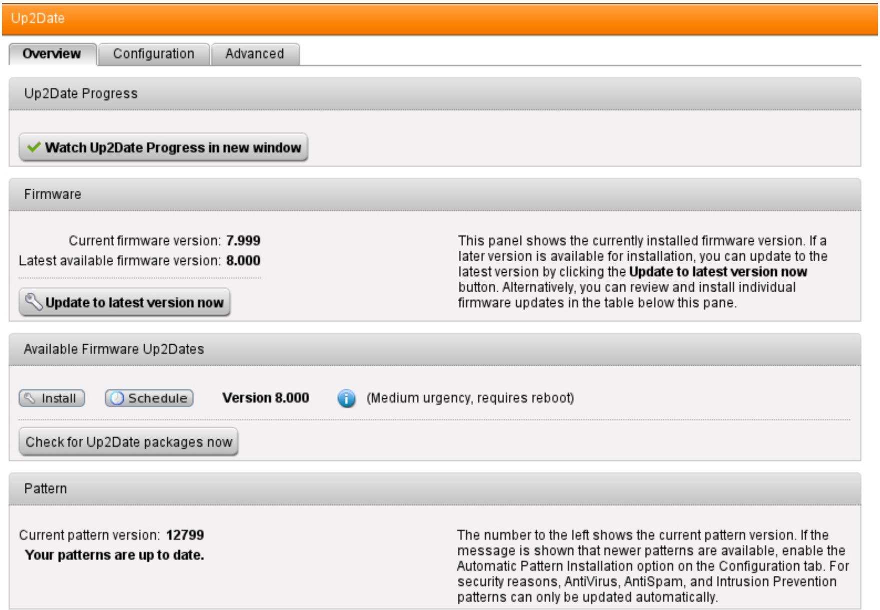


図17 Up2Date:【概要(Overview)】ページ

Up2Date進行状況(Up2Date Progress)

このセクションはインストールプロセスを開始した場合のみ表示されます。*【Up2Dateの進行状況を新しいウィンドウで確認する(Watch Up2Date Progress in New Window)】*ボタンをクリックして、更新の進行状況をモニタしてください。ブラウザでポップアップウインドウの表示を禁止していない限り、更新の進行状況を示す新しいウインドウが表示されます。表示されない場合は、ポップアップウインドウを明示的に許可する必要があります。

注 - インストールプロセスが開始する前に、標準バックアップEメール受信者にバックアップが送信されます。

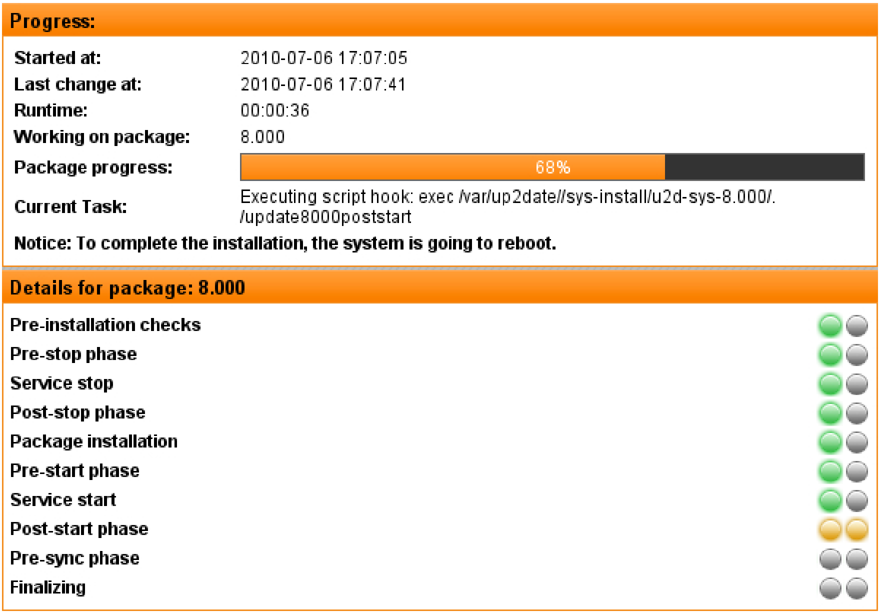


図18 Up2Date: 進捗ウィンドウ

ファームウェア(Firmware)

【*ファームウェア(Firmware)*】セクションには、現在インストールされているファームウェアのバージョンが表示されます。更新パッケージが利用できる場合は、【*すぐに最新バージョンに更新(Update to Latest Version Now)*】ボタンが表示されます。また、【*利用可能なファームウェアの概要(Available Firmware Up2Dates)*】セクションにメッセージが表示されます。ここで最新の更新パッケージを直接ダウンロードしてインストールできます。【*すぐに最新バージョンに更新(Update to Latest Version Now)*】をクリックすると、新しいウインドウに更新の進行状況が表示されます。これには、Webadminの【*リロード(Reload)*】ボタンをクリックします。

利用可能なファームウェアの概要(Available Firmware Up2Dates)

【*設定(Configuration)*】タブで【*手動(Manual)*】を選択すると、このセクションに【*すぐにUp2Dateパッケージを確認(Check for Up2Date Packages Now)*】ボタンが表示されます。このボタンを使用して、ファームウェアのUp2Dateパッケージを手動でダウンロードできます。Up2Dateが複数利用できる場合は、どれをインストールするかを選択できます。最新のバージョンを直接インストールする場合は、【*ファームウェア(Firmware)*】セクションで【*すぐに最新バージョンに更新(Update to Latest Version Now)*】ボタンを使用できます。

各Up2Dateには【*スケジュール(Schedule)*】ボタンがあり、更新パッケージを自動的にインストー

ルする日時を指定できます。スケジュールしたインストールを取り消す場合は、【*キャンセル(Cancel)*】をクリックします。

「暗黙的」インストールに関する注記:スケジュールしたUp2Dateパッケージが、古いUp2Dateパッケージを最初にインストールすることを必要とする場合があります。その場合、この古いUp2Dateパッケージは、実際のUp2Dateパッケージの前にインストールするよう自動的にスケジュールされます。このパッケージに特定のタイミングを指定することもできますが、そのインストールを止めることはできません。

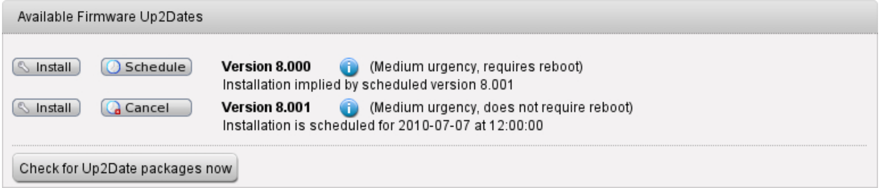


図19 Up2Date: Up2Dateパッケージの暗黙的インストール

パターン(Pattern)

【*パターン(Pattern)*】セクションには、インストールしたパターンの現在のバージョンが表示されます。【*設定(Configuration)*】タブで【*手動(Manual)*】を選択すると、【*すぐにパターンを更新(Update Patterns Now)*】ボタンが表示されます。このボタンを使用して、使用可能な新しいパターンをダウンロードしてインストールします。

注 - ユニットを正常に動作させるためには、現在のパターンバージョンと利用可能な最新のパターンバージョンが一致している必要はASGありません。お使いのユニットに新しいパターンを適用できない場合は、現在のパターンバージョンと利用できる最新パターンバージョンが異なってきます。どのパターンをダウンロードするかは、お客様の設定とハードウェアの構成によります。たとえば、Astaro Security Gatewayの侵入防止機能を使用しない場合は、新しく利用可能になったIPS パターンはインストールされません。このようにして、現在インストールされているパターンバージョンと利用できる最新のパターンバージョンの開きが大きくなっていきます。

4.4.2設定

デフォルトでは、新しい更新パッケージは自動的にゲートウェイにダウンロードされます。

ファームウェアのダウンロード間隔(Firmware Download Interval)

このオプションは、デフォルトで15分に設定されています。つまり、Astaro Security Gatewayは、15分毎に利用できるファームウェアの更新を確認します。Astaro Security Gateway は、利用できるファームウェア更新パッケージを自動的にダウンロードします(インストールは行いませ

ん)。これが行われる実際の時間は、選択された間隔の制限内でランダムに決定されます。最長で【*マンスリー(Monthly)*】の間隔を指定できます。または、ドロップダウンリストから【*手動(Manual)*】を選択することで、ファームウェアの自動ダウンロードを無効にできます。【*手動(Manual)*】を選択した場合は、【*すぐにUp2Dateパッケージを確認(Check for Up2Date Packages Now)*】ボタンが【*概要(Overview)*】タブに表示されます。

パターンのダウンロード/インストール間隔(Pattern Download/Installation Interval)

このオプションは、デフォルトで15分に設定されています。つまり、Astaro Security Gateway は、15分毎に利用できるパターンの更新を確認します。Astaro Security Gateway は、利用できるパターン更新パッケージを自動的にダウンロードしてインストールします。これが行われる実際の時間は、選択された間隔の制限内でランダムに決定されます。最長で【*マンスリー(Monthly)*】の間隔を指定できます。または、ドロップダウンリストから【*手動(Manual)*】を選択することで、パターンの自動ダウンロードとインストールを無効にできます。【*手動(Manual)*】を選択した場合は、【*すぐにパターンを更新(Update Patterns Now)*】ボタンが【*概要(Overview)*】タブに表示されます。

4.4.3詳細

【*マネジメント(Management)*】>>【*Up2Date*】>>【*詳細(Advanced)*】タブで、詳細なUp2Dateオプションを設定できます。たとえば、ゲートウェイ用に親プロキシまたはUp2Dateキャッシュを選択することなどができます。

注 - 更新パッケージはAstaroのFTP サーバからダウンロードできます。

手動Up2Dateパッケージアップロード(Manual Up2Date Package Upload): お使いのゲートウェイが新規更新パッケージを直接ダウンロードするためにインターネットまたはUp2Dateキャッシュに直接アクセスできない場合は、更新パッケージを手動でアップロードできます。手動でアップロードするには、以下の手順に従います。

1. ***【ファイルのアップロード(Upload File)】ダイアログボックスを開きます。***
   【*Up2Dateファイル(Up2Date File)*】ボックスの横にあるフォルダアイコンをクリックします。

   【*ファイルのアップロード(Upload File)*】ダイアログボックスが開きます。

2. **更新パッケージを選択します。**
   【*ファイルのアップロード(Upload File)*】ダイアログボックスの【*参照(Browse)*】をクリックして、アップロードする更新パッケージを選択します。

3. **【アップロード開始(Start Upload)】をクリックします。**
   更新パッケージがゲートウェイにアップロードされます。

4. **【適用(Apply)】をクリックします。**
   設定が保存されます。

親プロキシ(Parent Proxy)

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国で必要とされます。親プロキシの使用がセキュリティポリシで求められている場合、ここでホスト定義とポートを選択して親プロキシを設定できます。

親プロキシを使用(Use a Parent Proxy): このチェックボックスにチェックを入れて、親プロキシの使用を有効にします。プロキシのホスト名とポートを入力します。

このプロキシは認証が必要(This Proxy Requires Authentication): 親プロキシが認証を必要とする場合は、ここでユーザ名とパスワードを入力します。

親プロキシが設定されている場合は、Astaro Security Gateway はファームウェアとパターンのUp2Dateの両方を親プロキシからフェッチします。

4.5バックアップ/リストア

バックアップ/リストア機能を使用すると、ゲートウェイの設定をローカルディスク上のファイルに保存することができます。このバックアップファイルを使用すると、新しいシステムや設定が誤っているシステムに、適切であるとわかっている設定をインストールすることができます。

システムに変更を加えるたびに忘れずにバックアップをとってください。これにより、常に最新の設定を使用できるようになります。さらに、バックアップは安全な場所に保存してください。この理由は、証明書や暗号化鍵といったセキュリティ関連のデータも含まれているためです。バックアップの生成後、読み取り可能であることを必ずチェックしてください。外部プログラムを使用してMD5チェックサムを生成すると良いでしょう。これにより、バックアップの完全性を後でチェックすることができます。

4.5.1バックアップ/リストア

*【マネジメント(Management)】>>【バックアップ/リストア(Backup/Restore)】>>【バックアップ/リストア(Backup/Restore)】>*ページでは、バックアップの作成やインポートに加え、既存のバックアップのリストア、ダウンロード、送信、削除ができます。

>使用可能なバックアップ(Available Backups)

このセクションは、バックアップを1つ以上作成していないと表示されません。

すべてのバックアップが、作成日時、ASGバージョン番号、作成ユーザ、コメント付きでリストされます。

バックアップに対して、*リストア*、*ダウンロード*、*送信*、*削除*を実行できます。バックアップのダウンロードを選択すると、ダウンロードしたバックアップを保存するためのファイルシステムの場所を選択するプロンプトが表示されます。

【*送信(Send)*】をクリックすると、小さいダイアログウィンドウが開き、ファイルを暗号化して(パスワードとともに)送信するか、暗号化せずに送信するかを決めることができます。【*保存(Save)*】をクリックしてバックアップを送信します。受信者は標準受信者となります。つまり、【*自動バックアップ(Automatic Backups)*】タブに指定したアドレスに、バックアップが送信されます。

> **注 -**Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの【*インターネットオプション*】>>【*セキュリティ*】で設定します。さらに、Internet Explorer 7を使用する場合は、【*信頼済みサイトゾーン*】で【*ファイルのダウンロード時に自動的にダイアログを表示*】を選択します。

バックアップのダウンロードまたは送信の前に、バックアップを暗号化するオプションがあります。暗号化は、CBCモードではBlowfish暗号にって実現します。パスワードを入力します(確認のために2回入力します)。バックアップのインポート時に、このパスワードが求められます。暗号化されたバックアップのファイル拡張子は`ebf`、暗号化されていないバックアップのファイル拡張子は`abf`です)。

> **注 -** バックアップには、管理者パスワード、HAパスフレーズ(設定している場合)、すべてのRSA鍵およびX.509証明書が含まれます。これは機密情報なので、暗号化を有効にするのが賢明です。

USBスティックなどのFATフォーマットされたUSBフラッシュドライブから、暗号化されていないバックアップファイル(ファイル拡張子`abf`)をリストアすることもできます。USBフラッシュドライブからバックアップをリストアするには、バックアップファイルをUSBフラッシュドライブにコピーして、ブート(起動)前にデバイスをAstaro Security Gatewayにプラグインします。デバイスに複数のバックアップファイルが保存されている場合、辞書的に最初のファイルが使用されます(数字は文字より優先します)。たとえば、バックアップファイルである`gateway_backup_2007-04-17.abf`と`2006-03-20_gateway_backup.abf`の両ファイルがUSBフラッシュドライブに保存されているとします。ブート時

に使用されるのは2つ目のファイルです。このファイルはもう一方より日時が古いのですが、ファイル名の先頭が数字であるためです。

さらに、バックアップのリカバリが成功するとロックファイルが作成され、USBフラッシュドライブがまだプラグインされている間に同じバックアップが何度も繰り返しインストールされることを防ぎます。前のバックアップを再びインストールしたい場合には、USBフラッシュドライブをプラグインしていない状態でリブート(再起動)する必要があります。これにより、すべてのロックファイルが削除されます。再びUSBフラッシュドライブをプラグインしてからブートすると、同じバックアップをインストールすることができます。

バックアップの作成

バックアップは、(予期しない)変更または故障の後でシステムをリストアするために便利なだけではありません。類似の設定にするシステムをセットアップする際のテンプレートとして使用し、これらのシステムをあらかじめある程度設定しておくことで、時間を大幅に節約できます。そのためには、バックアップを作成する前に、ホスト名、証明書など特定の情報を削除しておくことができます。

現在のシステム状態のバックアップを作成するには、次の手順に従います。

1. **【*バックアップの作成(Create Backup)*】セクションに、コメントを入力します**(オプション)。
   コメントは、バックアップリストでバックアップとともに表示されます。

2. **次の設定を行います**(オプション)。
   ホスト固有のデータの削除(Remove host-specific data): ホスト固有のデータなしでバックアップを作成するには、このオプションを選択します。この対象となるのは、ホスト名、SNMPデータ、HAデータ、ログ管理データ、匿名パスワード、ならびにメールセキュリティ、Webセキュリティ、クライアント認証、IPsec、SSL VPN、RED、WebAdmin、Webアプリケーションファイアウォール、およびプロキシ用のすべての証明書、公開鍵と秘密鍵、および指紋とシークレットなどです。
   このようなバックアップは、類似のシステムを複数セットアップするために便利です。ただし、いくつか考慮すべき点があります。1) リストア後、基本システムセットアップが表示されます。2) 最初のインタフェースのみが設定されています。プライマリIPアドレスは、インストール中に構成される設定の1つです。

> **警告 -** ほとんどのホスト固有データが削除されても、このようなバックアップテンプレートにはユーザパスワードなどの機密情報がまだ含まれています。そのため、暗号化することをお勧めします。

管理メールメッセージの削除(Remove administrative mail addresses):ASGの様々な部分(メールセキュリティのポストマスタアドレス、通知など)で使用される管理者のEメールアドレスを追加で削除するには、このオプションを選択します。このオプションは、顧客のサイトでAstaro Security GatewayデバイスをセットアップするITパートナーにとって特に便利です。

3. ***【バックアップを今すぐ作成(Create Backup Now)】*をクリックします。**
   使用可能なバックアップのリストに、バックアップが表示されます。

バックアップのインポート(Import Backup)

バックアップをインポートするには、フォルダアイコンをクリックし、アップロードするバックアップファイルを選択してから、【*保存(Save*】をクリックしてください。暗号化されたバックアップファイルをインポートする場合、バックアップのインポート前に、正しいパスフレーズを入力する必要があります。バックアップはすぐにリストアされるのではなく、【使用可能なバックアップ(Available Backups)】*リストに追加されます。*

4.5.2自動バックアップ

*【マネジメント(Management)】>>【バックアップ/リストア(Backup/Restore)】>>【自動バックアップ(Automatic Backup)】*タブでは、バックアップの自動生成に関する複数のオプションを設定することができます。バックアップを自動的に作成するためには、次の手順に従います。

1. **【*自動バックアップ(Automatic Backups)*】タブで自動バックアップを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンが緑色になり、【*オプション(Options)*】および【*バックアップをEメール送信(Send Backups by E-mail)*】エリアが編集可能になります。

2. **間隔を選択します。**
   自動バックアップは、さまざまな間隔で作成することができます。

   デイリー、ウィークリー、マンスリーから選択できます。

3. **保存する最大バックアップ数を指定します。**
   ここで指定した数まで、バックアップが保存されます。最大値に到達すると、一番古いバックアップが削除されます。

   この対象となるのは、自動作成されたバックアップのみです。システム更新の前に手動で作成されたバックアップや自動的に作成されたバックアップは削除されません。

4. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

ゲートウェイのバックアップ作業を簡素化するために、バックアップ機能では、定義したEメールアドレスのリストに対して、バックアップファイルをEメールで送信することができます。

受信者(Recipients): 自動的に生成されたバックアップは、【*受信者(Recipients)*】ボックスに含まれるユーザに送信されます。複数のアドレスを追加できます。デフォルトでは、最初の管理者のEメールアドレスが使用されます。

Eメールバックアップの暗号化(Encrypt E-Mail Backups):さらに、オプションでバックアップを暗号化できます(3DES暗号化)。

パスワード(Password):【*暗号化(Encryption)*】このオプションを選択したら、パスワードを入力します(確認のために2回)。バックアップのインポート時に、このパスワードが求められます。

自動的に作成されたバックアップは、*作成者*を示す【システム(`System`)】フラグ付きで【*バックアップ/リストア(Backup/Restore)*】タブの【*使用可能なバックアップ(Available Backups)*】リストに表示されます。ここで、自分で作成したバックアップと同様に、リストア、ダウンロード、削除を実行できます。

4.6ユーザポータル

Astaro Security Gatewayのユーザポータルは、許可されたユーザにパーソナルなEメールおよびリモートアクセスサービスを提供するユニットの特別なブラウザベースアプリケーションです。ユーザポータルにアクセスするには、Astaro Security GatewayのURL(`https://192.168.2.100`など)をブラウズします(HTTPSプロトコルを使用していることと、WebAdminインタフェースにアクセスするために通常入力するポート番号`4444`がないことに注意)。

ユーザポータルは、Eメール隔離を始めとする機能を備えています。Eメール隔離は、悪意あるソフトウェアに感染したメッセージ、不審な添付物を含むメッセージ、スパムと特定されたメッセージ、または明確に禁止した表現を含むメッセージを保持します。

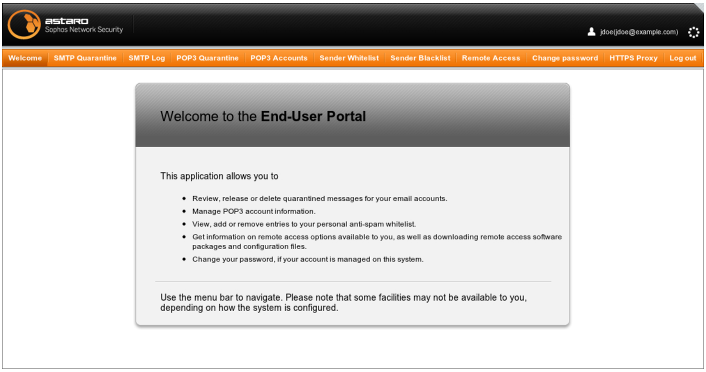


図20 ユーザポータル:「ようこそ」のページ

ユーザポータルで、ユーザは以下のサービスにアクセスできます。

- **SMTP隔離(SMTP Quarantine)**:ユーザは隔離場所に保持されているメッセージを表示したりリリースできます。どのタイプのメッセージをユーザがリリースできるかは【*メールセキュリティ(Mail Security)*】>>【*隔離レポート(Quarantine Report)*】>>【*詳細(Advanced)*】タブで決定できます。(このタブは、POP3が無効な場合は【*メール隔離(Mail Quarantine)*】となります。)
- **SMTPログ(SMTP Log)**:ここでは、ユーザはメールトラフィックのSMTPログを表示できます。(このタブは、POP3が無効な場合は【*メールログ(Mail Log)*】となります。)
- **POP3隔離(POP3 Quarantine)**: ユーザは隔離場所に保持されているメッセージを表示したりリリースできます。どのタイプのメッセージをユーザがリリースできるかは【*メールセキュリティ(Mail Security)*】>>【*隔離レポート(Quarantine Report)*】>>【*詳細(Advanced)*】タブで決定できます。(このタブは、SMTPが無効な場合は【*メール隔離(Mail Quarantine)*】となります。)
- **POP3アカウント(POP3 Accounts)**:ユーザは使用するPOP3アカウントの資格情報を入力できます。POP3アカウントの資格情報が与えられたスパムメールのみがユーザポータルに表示されます。POP3アカウントの資格情報が保存されているユーザは、各Eメールアドレスについて個々の隔離レポートを受け取ります。許可されるPOP3サーバは【*メールセキュリティ(Mail Security)*】>>【*POP3*】>>【*詳細(Advanced)*】タブで指定する必要があります。
- **送信者ホワイトリスト(Sender Whitelist)**:ここで送信者をホワイトリストに追加することで、それらの送信者から送信されたメッセージがスパムとして分類されないようにできます。ホワイトリスト内の送信者は、有効なEメールアドレス(例:`jdoe@example.com`)またはア

スタリスクをワイルドカードとして使用して特定ドメインの全Eメールアドレス(例:`*@example.com`)を指定できます。

- **送信者ブラックリスト(Sender Blacklist)**:ここでEメール送信者をブラックリストに追加する(例:`phishing@hotmail.com`)か、ドメイン全体をブラックリストに追加する(例:`*@hotmail.com`)ことができます。ブラックリストは、システム内でSMTPとPOP3が使用されていれば、SMTPとPOP3の両方のEメールに適用されます。新しいエントリを指定するには、「+」アイコンをクリックしてアドレスを入力し、チェックアイコンをクリックして保存します。
- **リモートアクセス(Remote Access)**:ユーザはリモートアクセスクライアントソフトウェアおよびそれらに付属する設定ファイルをダウンロードできます。ただし、*【リモートアクセス(Remote Access)】*タブは、その特定ユーザに対して最低1つのリモートアクセスモードが有効になっている場合のみ利用できます。

> **注 -**Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの*【インターネットオプション】*>>*【セキュリティ】*で設定します。さらに、Internet Explorer 7を使用する場合は、*【信頼済みサイトゾーン】*で*【ファイルのダウンロード時に自動的にダイアログを表示】*を選択します。

- **パスワードの変更(Change Password)**:ユーザはユーザポータルにアクセルするためのパスワードを変更できます。
- **Webフィルタ(Web Filter)**:ユーザはWebフィルタCA証明書をインポートし、セキュアWebサイトへの訪問時に表示されるエラーメッセージを回避することができます。*【プロキシCA証明書をインポート(Import Proxy CA certificate)】*をクリックすると、ユーザのブラウザに、他の目的に対してCAを信頼するか確認するプロンプトが表示されます。詳しくは、「*Webセキュリティ*」>>「*Webフィルタ*」>>「*HTTPS CA*」の章を参照してください。
- **ログアウト(Log Out)**:ユーザポータルからログアウトするには、ここをクリックします。これは、ログイン時に*【ログインを記憶(Remember My Login)】*を選択した場合に(これによりクッキーが作成されます)、明示的にログアウトしてこのクッキーを削除したいときのみ必要です。そうでない場合は、このログアウトボタンを使用する必要はありません。ブラウザのタブまたはウインドウを閉じるだけで十分です。

4.6.1グローバル

【マネジメント(Management)】>>*【ユーザポータル(User Portal)】*>>*【グローバル(Global)】*タブで、ユーザポータルを有効化できます。さらに、ユーザポータルへのアクセスを許可するネットワークとユーザを指定できます。

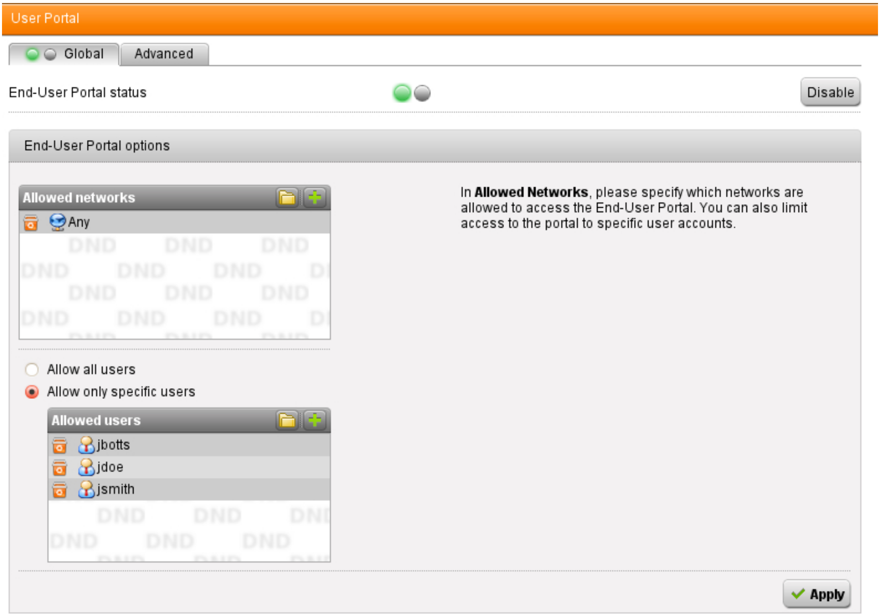


図21 ユーザポータル: ユーザポータルへのアクセスの設定

ユーザポータルへのアクセスを有効にするには、以下の手順に従います。

1. **ユーザポータルを有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり*【ユーザポータルオプション(User Portal Options)】*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   ユーザポータルへのアクセスを許可するネットワークを選択します。

3. **許可するユーザを選択します。**
   ユーザポータルへのアクセスを許可するユーザまたはユーザグループを選択します。

   すべてのユーザにアクセスを許可しない場合は、*【特定のユーザのみ許可(Allow Only Specific Users)】*をクリックし、ユーザとユーザグループを個々に選択します。

4. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

4.6.2詳細

【*詳細(Advanced)*】タブで、ユーザポータルの代替ホスト名とポート番号に加え、言語とセキュリティオプションを設定できます。

言語(Language)

ログイン時に、ユーザポータルはWebブラウザの言語設定をフェッチし、それぞれのロケールをロードして、ブラウザのデフォルトと同じ言語でポータルを表示します。ブラウザの言語設定がユーザポータルで利用できない場合は、フォールバック(予備)の言語をここで選択できます。

【セキュリティ(Security)】

ユーザポータルはCookieを使用してセッションを追跡します。永続的(固定)Cookieにより、セッションを閉じた後で再度ログインしないで戻ることが可能になります。これらはいつでもユーザ側で削除できますが、ユーザポータルの【*ログアウト(Log Out)*】ボタンを使用することが必要です。

ポータルアイテムの無効化(Disable Portal Items)

ここにリストされているそれぞれの機能をWebAdminで有効にすると、ユーザポータルにメニュー項目が表示されます。ただし、ここでは、ユーザポータルで表示*しない*メニュー項目を定義できます。これを定義するには、それぞれのオプションを選択して【*適用(Apply)*】をクリックします。

ネットワーク設定(Network Settings)

ホスト名(Hostname): デフォルトでは、これはゲートウェイのホスト名です(【*マネジメント(Management)*】>>【*システム設定(System Settings)*】>>【*ホスト名(Hostname)*】タブで指定)。ただし、インターネットを介してアクセスするユーザにユーザポータルへのアクセスを付与する場合は、パブリックに解決できる代替ホスト名をここに入力する必要があります。

リスンアドレス(Listen Address): デフォルトは【*すべて(Any)*】です。Webアプリケーションファイアウォールを使用する場合、サービスがユーザポータル接続をリスンするためのインタフェースアドレスを指定する必要があります。ユーザポータル接続ハンドラとWebアプリケーションファイアウォールが受信SSL接続を識別できるようにするために、この設定が必要です。

ポート(Port): デフォルトでは、HTTPSのポート`443`が選択されています。ポートは、`80`、または`1024`～`65535`の任意の値に変更できます。`10443`または*WebAdmin TCPポート*は選択できません。これは【*マネジメント(Management)*】>>【*WebAdmin設定(WebAdmin Settings)*】>>【*一般(General)*】タブで設定されています。

ようこそメッセージ(Welcome Message)

ユーザポータルのようこそメッセージをカスタマイズできます。シンプルなHTMLマークアップとハイパーリンクを使用できます。

注 – 家庭用ライセンスを使用している場合は、ようこそメッセージを変更できません。

4.7通知

Astaro Security Gateway には、ゲートウェイで発生するあらゆる種類のセキュリティ関連イベントについて、EメールまたはSNMPトラップで即時通知する機能が搭載されています。管理者が知るべきすべてのイベントが、各種エラー、警告、情報コードによって示されます。どのような通知が送信されるのかは、*【通知(Notifications)】*タブで設定した選択内容に応じて決まります。

4.7.1グローバル

*【マネジメント(Management)】>>【通知(Notifications)】>>【グローバル(Global)】*タブでは、ゲートウェイが送信する通知Eメールに利用される送信者アドレス(つまり*送信元(From)*アドレス)を設定できます。デフォルトでは`do-not-reply@fw-notify.net`となっています。このアドレスを変更する場合、お客様のドメインのEメールアドレスを入力することをお勧めします。この理由は、一部のメールサーバでは、指定された送信者アドレスが本当に存在することを確認するように設定されているためです。

さらに、ゲートウェイ通知の受信者を指定することができます。デフォルトでは、初期セットアップ時に入力された管理者のEメールアドレスです。

通知を制限(Limit Notifications): 一部のセキュリティ関連イベント(検出された侵入試行など)では、大量の通知が発生し、通知受信者の受信トレイが短時間でいっぱいになる可能性があります。このため、Astaro Security Gatewayには、1時間あたりに送信される通知数を制限するための妥当なデフォルト値が用意されています。このオプションを無効にすると、*【マネジメント(Management)】>>【通知(Notifications)】>>【通知(Notifications)】*タブで通知を送信するように設定されているすべてのセキュリティ関連のイベントから通知が発生します。

デバイス固有のテキスト(Device Specific Text)

ここでは、Astaro Security Gatewayの説明(場所など)を入力できます。この情報は、送信される通知に示されます。

4.7.2通知

通知は次の3つのカテゴリに分類されます。

- **CRIT**: ゲートウェイが操作不能になる可能性がある重大なイベントを通知するメッセージ。
- **WARN**: しきい値の超過など、ユーザの注意を必要とする潜在的な問題についての警告。
- **INFO**: システムコンポーネントの再起動など、情報提供目的のみのメッセージ。

通知をEメールとSNMPトラップのいずれで送信するかを選択できます。

4.7.3詳細

ASGでEメールを直接送信できない場合、Eメールを送信するスマートホストを設定することができます。次の手順で実行します。

1. ***【マネジメント(Management)】>>【通知(Notifications)】>>【詳細(Advanced)】*タブで*【外部SMTP(External SMTP)】*を有効化します。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。
2. **スマートホストを入力します。**
   ドラッグ＆ドロップを使用できます。ポートは、デフォルトのSMTPポートである25に事前設定されています。
   - **TLSを使用(Use TLS)**: 通知の送信でTLSを強制するには、このチェックボックスにチェックを入れます。スマートホストでTLSがサポートされない場合、通知は送信されません。
3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

スマートホストで認証が必要な場合、下の*【認証(Authentication)】*エリアでスマートホスト用の対応するユーザ名とパスワードを入力してください。設定を保存するには*【適用(Apply)】*をクリックします。

4.8カスタマイズ

*【マネジメント(Management)】>>【カスタマイズ(Customization)】*メニューのタブを使用すると、Astaro Security Gatewayが生成するステータスメッセージとEメール通知のテンプレートをカスタマイズおよびローカライズして、会社のポリシやコーポレートアイデンティティに合わせてこれらのメッセージを調整することができます。

注 – 家庭用ライセンスを使用している場合は、カスタマイズできません。

4.8.1グローバル

*【マネジメント(Management)】>>【カスタマイズ(Customization)】>>【グローバル(Global)】*タブでは、ユーザに表示されるシステムメッセージのグローバル表示オプションをカスタマイズすることができます。UTF-8/Unicodeがサポートされています。

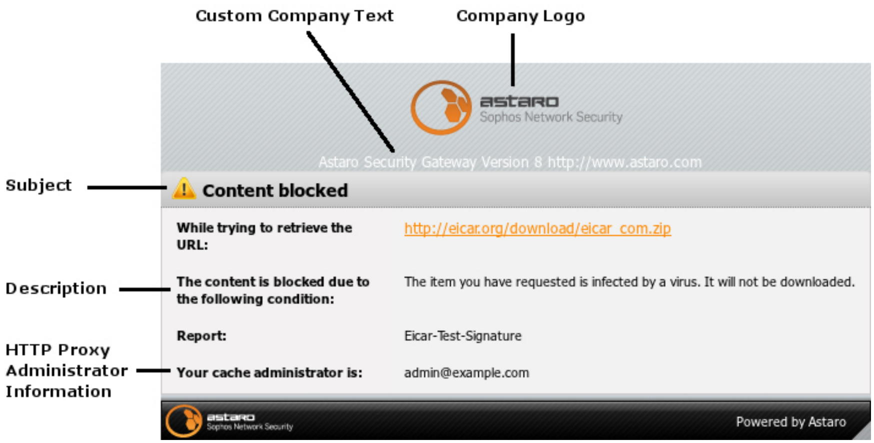


図22 カスタマイズ:ブロックされるページの例とカスタマイズ可能な部分

会社のロゴ(Company Logo)

会社のロゴ/バナーをアップロードし(jpg形式のみ)、次の状況で使用することができます。

- Webフィルタメッセージ
- 「POP3メッセージがブロックされました」メッセージ

- (隔離レポートを通じてスパムメールが隔離場所からリリースまたはホワイトリスト化された後で表示される)隔離リリースステータスメッセージ
- 隔離レポート

画像の解像度は適度な値に制限してください(100 x 200ピクセルなど)。

バナーをアップロードするには、次の手順に従ってください。

1. ***【ファイルのアップロード(Upload File)】ダイアログボックスを開きます。***
   【*新しいロゴのアップロード(Upload New Logo)*】ボックスの横にあるフォルダアイコンをクリックします。

   【*ファイルのアップロード(Upload File)*】ダイアログボックスが開きます。

2. **バナーを選択します。**
   アップロードするバナーがある場所までブラウズします。

   バナーを選択し、【*保存(Save)*】をクリックします。

3. **【*適用(Apply)*】をクリックします。**
   バナーがアップロードされ、すでにインストールされているファイルと置き換えられます。

カスタムカンパニーテキスト(Custom Company Text)

Astaro Security Gatewayのウイルススキャナまたはコンテンツフィルタによって Webサイトがブロックされたときに、会社ロゴの下に表示されるメッセージをカスタマイズします。ここには、管理者の連絡先データなどを入力することができます。Webサイトは、さまざまな理由でブロックされます。たとえば、このWebサイトが禁止カテゴリに属している場合やスパイウェアとして分類されている場合、あるいは危険だとみなされる拡張子のファイル(実行可能ファイルなど)をユーザがダウンロードしようとした場合などです。これらの状況で使用されるテンプレートを、【*マネジメント(Management)*】>>【*カスタマイズ(Customization)*】>>【*Webフィルタ(Web Filter)*】タブで変更することができます。

4.8.2Webフィルタ

Astaro Security GatewayのWebフィルタの警告Webページ用のテンプレートをカスタマイズします。この警告Webページは、禁止されたWebサイトへのアクセスが検知されると表示されるもので、それぞれの違反タイプに対する警告文を示します。これらのテンプレートを他の言語に翻訳したり、顧客サポートの連絡先情報が表示されるように変更したりできます。次のメッセージテンプレートをカスタマイズできます。

- **Webフィルタ管理者情報(Web Filtering Administrator Information)**:ここで、Webフィルタを管理する管理者についての情報を入力できます。さらに、管理者のE

メールアドレスも入力可能です。

- **サーフプロテクションによってブロックされたコンテンツ(Content Blocked by Surf Protection)**: このメッセージは、ブロック対象として設定されているURLカテゴリと一致するコンテンツを持つWebページにユーザがアクセスしようとすると表示されます。
- **ブラックリストによってブロックされたコンテンツ(Content Blocked by Blacklist)**: このメッセージは、ブラックリスト化されたブラックリストのURLと一致するコンテンツを持つWebページをユーザが取得しようとすると表示されます。URLをブラックリスト化する方法は、*「Webセキュリティ」>>「Webフィルタ」>>「URLフィルタリング」*を参照してください。
- **検出されたウイルス(Virus Detected)**: このメッセージは、ウイルス感染が原因でファイルがブロックされた場合に表示されます。
- **ファイルダウンロード中(Downloading File)**: このメッセージは、ファイルのダウンロードの進行中に表示されます。
- **ウイルススキャン中(Virus Scanning)**: このメッセージは、悪意のあるコンテンツが含まれていないかファイルをスキャンしているときに表示されます。
- **ファイルダウンロード完了(File Download Completed)**: このメッセージは、ファイルのダウンロードとスキャンが完了した後で表示されます。
- **認証付き透過モード(Transparent Mode with Authentication)**: このセクションは、【*認証付き透過モード(Transparent Mode with Authentication)*】でWebフィルタを使用しているときに限って有効です。テキストは認証ページに表示されます。各ユーザはWebフィルタを使用する前にこの認証ページにログインする必要があります。【*利用条件(Terms of Use)*】フィールドはデフォルトで空になっています。つまり、認証ページには免責事項が表示されません。ユーザが同意する必要がある免責事項を追加するには、このフィールドに記入します。【*利用条件(Terms of Use)*】フィールドを空にすると、免責事項が再び無効になります。
- **URLフィルタの上書き(URL Filter Override)**: このメッセージは、ページがブロックされ、各ユーザに対してバイパスブロックオプションが有効担っている場合に表示されます(*「Webセキュリティ」>>「Webフィルタリング」>>「URLフィルタリング」*を参照)。

4.8.3ダウンロードマネージャ

Webフィルタが有効である場合、サイズが1 MBを超え、コンテンツタイプがテキストまたは画像以外であるコンテンツのダウンロード中、Webブラウザに次のダウンロードページが表示されます。要求されているのが動画または音声ストリームである場合や、5秒以内にファイルの50%超のダウンロードが完了している場合には、ダウンロードページは表示されません。

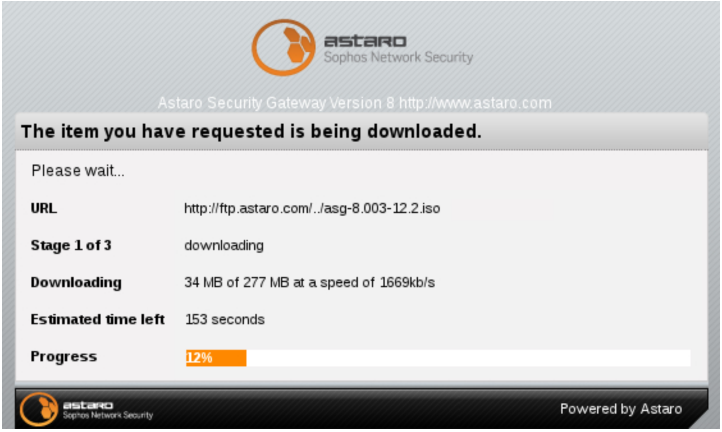


図23 カスタマイズ:HTTPダウンロードページ、ステップ1/3

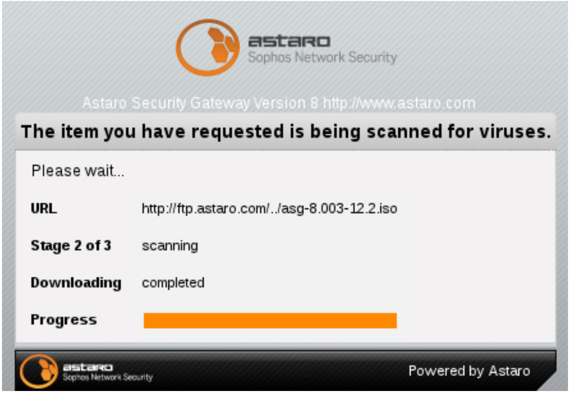


図24 カスタマイズ:HTTPダウンロードページ、ステップ2/3

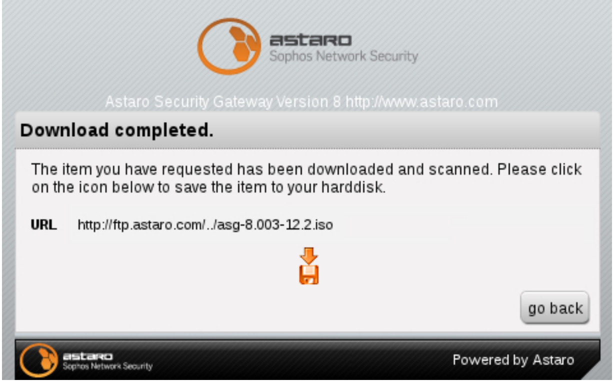


図25 カスタマイズ:HTTPダウンロードページ、ステップ3/3

4.8.4SMTP/POP3プロキシ

Astaro Security GatewayのSMTP/POP3プロキシによって生成されるユーザメッセージに使用されるテンプレートをカスタマイズします。これらのテンプレートを他の言語に翻訳したり、顧客サポートの連絡先情報が表示されるように変更したりできます。次のメッセージテンプレートをカスタマイズできます。

- **メッセージが隔離からリリースされました(Message Released From Quarantine)**: このメッセージは、Eメールが隔離から正常にリリースされたときに表示されます。
- **メッセージを隔離からリリースする際にエラーが発生しました(Error While Releasing Message From Quarantine)**: このメッセージは、メッセージを隔離からリリースする際にエラーが発生したときに表示されます。
- **POP3メッセージがブロックされました(POP3 Message Blocked)**: このメッセージは、POP3 Eメールがブロックされたときに受信者に送信されます。

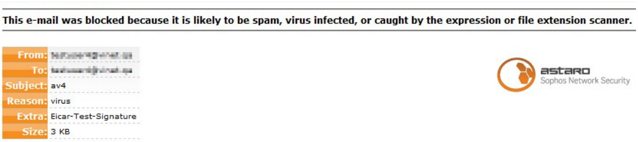


図26 カスタマイズ:POP3プロキシのブロックメッセージ

4.9SNMP

簡易ネットワーク管理プロトコル(SNMP)は、ルータ、サーバ、スイッチなどのネットワークに接続されたデバイスを監視するためにネットワーク管理システムで使用されます。SNMPによって管理者は、監視している各ネットワークデバイスの状態に関するクエリを速やかに実行できます。Astaro Security Gatewayは、SNMPクエリに返答したり、SNMPトラップをSNMP管理ツールに送信するように設定できます。前者は「管理情報ベース(*management information bases*:MIB)」によって実現します。MIBは、どのネットワークデバイスに対してどの情報がクエリ可能かを指定します。Astaro Security Gateway は、SNMPバージョン2と3および以下のMIBをサポートしています。

- **DISMAN-EVENT-MIB**: イベント管理情報ベース
- **HOST-RESOURCES-MIB**: ホストリソース管理情報ベース
- **IF-MIB**: インタフェースグループ管理情報ベース
- **IP-FORWARD-MIB**: IPフォワーディングテーブル管理情報ベース
- **IP-MIB**: *インターネットプロトコル*(IP)用管理情報ベース
- **NOTIFICATION-LOG-MIB**: 通知ログ管理情報ベース
- **RFC1213-MIB**: TCP/IPベースのインターネットのネットワーク管理用管理情報ベース:MIB II
- **SNMPv2-MIB**: *簡易ネットワーク管理プロトコル*(SNMP)用管理情報ベース
- **TCP-MIB**: *伝送制御プロトコル*(TCP)用管理情報ベース
- **UDP-MIB**: *ユーザデータグラムプロトコル*(UDP)用管理情報ベース

Astaro Security Gatewayシステム情報を取得するには、最低でもRFC1213-MIB(MIB II)をコンパイルしたSNMPマネージャを使用する必要があります。

4.9.1クエリ

*【マネジメント(Management)】>>【SNMP】>>【クエリ(Query)】*ページでは、SNMPクエリの使用を有効化できます。

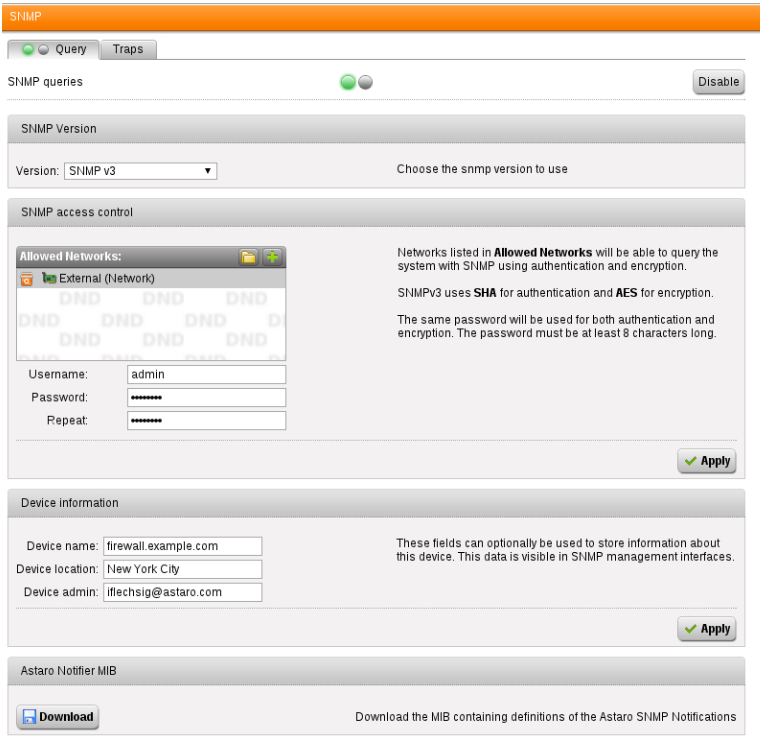


図 27 SNMP: SNMPクエリの設定

SNMPクエリを設定するには、次の手順に従ってください。

1. **【*SNMPクエリ(SNMP Queries)*】を有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   【*SNMPバージョン(SNMP Version)*】および【*SNMPアクセスコントロール(SNMP Access Control)*】セクションが編集可能になります。

2. **SNMPバージョンを選択します。**
   【*SNMPバージョン(SNMP Version)*】セクションで、ドロップダウンリストからバージョンを選択します。SNMPバージョン3には認証が必要です。

3. **許可されるネットワークを選択します。**

【*許可ネットワーク(Allowed Networks)*】ボックスにリストされているネットワークは、当製品上で実行されているSNMPエージェントにクエリを行うことができます。Astaro Security Gateway. アクセスは常に読み取り専用です。

- **コミュニティ文字列(Community String)**:バージョン2を使用する場合、コミュニティ文字列を入力します。SNMPコミュニティ文字列はパスワードとして機能し、SNMPエージェントへのアクセスを保護します。デフォルトでは、SNMPコミュニティ文字列は"public"に設定されていますが、お客様のニーズに応じて変更できます。

  注 - コミュニティ文字列に使用できる文字:(a～z)、(A～Z)、(0～9)、(+)、(_)、(@)、(.)、(-)、(空白)

- **ユーザ名/パスワード(Username/Password)**:バージョン3を使用する場合、認証が必要です。ユーザ名とパスワード(確認のために2回)を入力し、リモート管理者がクエリを送信できるようにします。パスワードは8文字以上にする必要があります。SNMP v3では、認証にSHAを、暗号化にAESを使用します。ユーザ名とパスワードはその両方で使用されます。

4. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

さらに、ゲートウェイについての追加情報を入力できます。

デバイス情報(Device Information)

【*デバイス情報(Device Information)*】テキストボックスに、名前、場所、管理者など、ゲートウェイに関する追加情報を指定できます。この情報は、SNMP管理ツールが読み取って、ゲートウェイの識別に使用します。

注 -ゲートウェイと【*許可ネットワーク(Allowed Networks)*】間のすべてのSNMPトラフィック(プロトコルバージョン2)は暗号化されず、パブリックネットワーク上での転送中に読むことができます。

Astaro Notifier MIB

このセクションで、Astaro notifierMIB をダウンロードできます。これには、通知トラップの現在の設定に基づいたAstaro SNMP通知の定義が含まれます。

4.9.2トラップ

*【トラップ(Traps)】*タブで、ゲートウェイで発生した関連イベントの通知をSNMPトラップとして送信する宛先のSNMPトラップサーバを定義できます。これらのトラップを表示するには、特別なSNMPモニタリングソフトウェアが必要です。

SNMPトラップとして送られるメッセージには、オブジェクト識別子(OID)が含まれます。たとえば、`.1.3.6.1.4.1.9789`が挙げられます。これは、IANAが発行した私企業番号に属します。`.1.3.6.1.4.1`は`iso.org.dod.internet.private.enterprise`プレフィックスで、`9789`はAstaroの私企業番号です。通知イベントのOIDは`1500`で、それに通知タイプのOIDおよび対応するエラーコード(`000`～`999`)が追加されます。以下の通知タイプを使用できます。

- `DEBUG = 0`
- `INFO = 1`
- `WARN = 2`
- `CRIT = 3`

例：通知「INFO-302:新しいファームウェアUp2Dateがインストールされました(New firmware Up2Date installed)」では、OID `.1.3.6.1.4.1.9789.1500.1.302`を使用し、以下の文字列が割り当てられます。

`[<HOST>][INFO][302]`

`<HOST>`はプレースホルダでシステムのホスト名を表し、通知の件名フィールドのタイプおよびエラーコードのみが伝送されます。

SNMPトラップサーバを選択するには、以下の手順に従います。

1. **【新規SNMPトラップシンク(New SNMP Trap Sink)】をクリックします。**
   *【新規SNMPトラップシンクの作成(Create New SNMP Trap Sink)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ホスト(Host): SNMPトラップサーバのホスト定義。

   コミュニティ文字列(Community string):SNMPコミュニティ文字列はパスワードとして機能し、クエリを行うSNMPメッセージへのアクセスを保護します。デフォルトでは、SNMPコミュニティ文字列は"public"に設定されています。それをリモートSNMPトラップサーバで設定された文字列に変更します。

> **注 -** コミュニティ文字列に使用できる文字:(a～z)、(A～Z)、(0～9)、(+)、(_)、(@)、(.)、(-)、(空白)

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいSNMPトラップサーバが*【トラップ(Traps)】*タブに表示されます。

4.10集中管理

*【集中管理(Central Management)】*メニューのページを使用すると、ゲートウェイのモニタリングやリモート管理に使用できる管理ツールへのインタフェースを設定することができます。

4.10.1 Astaro Command Center

Astaro Command Center(ACC)とは、Astaroの一元(集中)管理用製品です。モニタリング、設定、メンテナンス、インベントリなどの機能があり、管理者を複数設定することができます。この製品は、Astaroの各ゲートウェイソフトウェアおよびアプライアンスの状態、そのバージョン、現在の負荷、ライセンス期限、重大なセキュリティイベントを概要的に示すことを目的としています。希望する場合、2つ目のACCサーバを設定することができます。これは、設定を自力で行い(1つ目のACCサーバ)、マシンについては引き続きサードパーティ(MSSPなどによってモニタリングしたい(2つ目のACCサーバ)場合に便利です。

情報へのアクセスにはWebベースのグラフィカルフロントエンドを使用します。このフロントエンドには、モニタリング対象の全デバイスに対するさまざまな表示オプションが用意されています。さらに、ACCには各デバイスを自動的にトラッキング(追跡)するインベントリシステムが含まれています。最後に、さまざまな管理者権限を複数の管理者に割り当てることができるため、ACCはAstaroパートナーやMSSPにとって完璧なソリューションとなります。Astaro Command Centerについて詳しくは、Astaro Webサイトで提供されているACCデータシートをご確認ください。

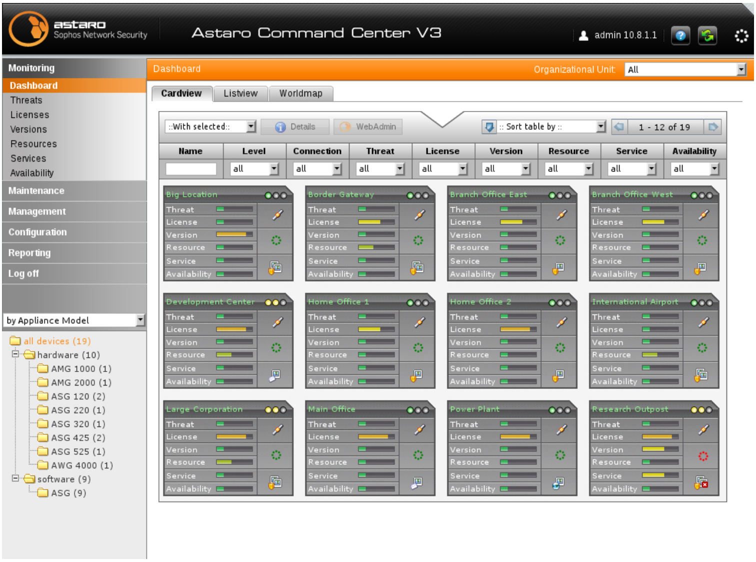


図28 集中管理 : Astaro Command Centerのダッシュボード

ACCの設定

Astaro Security GatewayがACCサーバのモニタリング対象になるよう準備するには、次の手順に従ってください。

1. **【*Astaro Command Center*】タブでACCを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色になり、【*ACC設定(ACC Settings)*】エリアが編集可能になります。

2. **【*ACCホスト(ACC Host)*】を指定します。**
   Astaro Security Gatewayの接続先とするACCサーバを選択または追加します。

   - **【認証(Authentication)】(オプション): ACCで認証が必要な場合、このオプションを選択して、ACCサーバで設定したものと同じパスワード(**共有シークレット)*を入力します。*

   - **Up2DateキャッシュとしてACCサーバを使用します**(オプション)。Up2Dateパッケージは、ACCサーバにあるキャッシュからフェッチすることができます。ゲートウェイ用にこの機能を使用するには、【*ACCサーバをUp2Dateキャッシュとして使用(Use ACC Server as Up2Date Cache)*】オプションを選択します。管理を行うACCの

管理者が、サーバ上でUp2Dateキャッシュ機能を適切に有効にしていることを確認してください。Up2Dateキャッシュ機能の使用は、Up2Datesのペアレントプロキシの使用と相互排他的になります。

選択したACCの管理者による管理を、ASGのどの機能エリアに対して許可するのか決定するには、4つのオプションがあります。これらのオプションには、ACCの管理機能が反映されています。詳細はACCのマニュアルを参照してください。2つ目のACCには設定オプションがありません。これは、デバイスの設定は1つ目のACCのみで可能であるためです。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。設定後すぐに、ここで選択したACCサーバでAstaro Security Gateway をモニタリングおよび管理できるようになります。

> **注 -** ゲートウェイとACCの間の通信はポート`4433`で行われますが、Astaro Command Centerには、HTTPSプロトコルを使用してブラウザ経由でアクセスすることができます。WebAdminの場合はポート`4444`、ゲートウェイマネージャインタフェースの場合はポート`4422`です。

図29 集中管理:ACC V2サーバの使用

ACCの健全性

*【ACCの健全性(ACC Health)】*セクションで、現在の接続ステータスと健全性を確認することができます。ページをリロードすると、このデータが更新されます。

ACCオブジェクト

このエリアは、ACC経由で作成されたオブジェクトがあり、このACCがAstaro Security Gatewayから切断されている場合を除き、無効になっています(グレーアウト表示されています)。ACCで作成されたオブジェクトとは、ネットワーク定義、リモートホスト定義、IPsec VPNトンネルなどです。

*【オブジェクトのクリーンアップ(Cleanup Objects)】*ボタンを押すと、デバイスを以前に管理していたACCで作成されたすべてのオブジェクトをリリースすることができます。これらのオブジェクトは通常ロックされ、ローカルデバイスのみで表示できます。このボタンを押すと、オブジェクトは完全にアクセス可能になり、ローカル管理者が再利用または削除できます。

> **注 -** 以前にACCで作成されたオブジェクトをクリーンアップすると、同じACCに再接続したときにこれらのオブジェクトを再変換できなくなります。つまり、リモートACCが、後で接続を再確立するデバイス用にオブジェクト定義をまだホストしている場合、ローカルコピーがすでに存在しても、これらのオブジェクトはデバイスに再配備されます。

ライブログ

ライブログを使用して、Astaro Security GatewayとACCの間の接続をモニタリングすることができます。【*ライブログを開く(Open Live Log)*】ボタンをクリックすると、新しいウィンドウでライブログが開きます。

4.11冗長化(HA)

インターネットセキュリティシステムの障害の主な原因は、ハードウェアの故障です。システムに障害が発生した後もサービスを継続して提供する能力をフェイルオーバーと呼びます。Astaro Security GatewayはHAフェイルオーバーを実現するため、お客様はプライマリシステムで障害が発生したときのためにホットスタンバイシステムをセットアップできます(active-passive)。あるいは、Astaro Security Gatewayを使用してクラスタをセットアップして、専用のネットワークトラフィックを一群のノードに分散させて運用し(active-active)、リソース利用率を最大限に高めて演算時間を削減することができます。これは従来の負荷分散アプローチと似ています。

Astaro Security Gatewayに導入された*冗長化*と*クラスタ*の概念には、密接な関係があります。HAシステムは2ノードクラスタと考えることができます。これは冗長性を実現する最低限の要件です。

クラスタ内の各ノードは次のいずれかの役割を果たすことができます。

- **マスタ**: ホットスタンバイ/クラスタセットアップ内のプライマリシステム。クラスタ内で、マスタはデータの同期と配信を行う責任を担います。
- **スレーブ**: ホットスタンバイ/クラスタセットアップ内のスタンバイシステム。マスタに障害が発生すると、オペレーションを引き継ぎます(テイクオーバーします)。
- **ワーカ**: データ処理のみを担当するシンプルなクラスタノード。

すべてのノードは、いわゆるハートビート信号を使用して自らをモニタリングします。ハートビート信号とは、他のノードが稼働していることを確認するために定期的に送信されるマルチキャストUDPパケットです。技術的エラーが原因で、いずれかのノードがこのパケットの送信に失敗すると、そのノードは*デッド(Dead)*と宣言されます。失敗したノードが担っていた役割に応じて、セットアップの構成が次のように変更されます。

- マスタノードで障害が発生した場合、スレーブがマスタの役割を引き継ぎ、IDが最も高いワーカノードがスレーブとなります。
- スレーブノードで障害が発生した場合、IDが最も高いワーカノードがスレーブとなります。

- ワーカノードで障害が発生した場合、処理能力が失われることによるパフォーマンス低下は認識されますが、フェイルオーバー機能は損なわれません。

レポーティング

すべてのレポーティングデータはマスタノード上で統合され、5分間隔で他のクラスタノードと同期されます。したがって、引き継ぎが発生すると、5分以下のレポーティングデータが失われます。ただし、データ収集プロセスには違いがあります。*【ログおよびレポーティング(Logging & Reporting)】>>【ハードウェア(Hardware)】*タブに表示されるグラフには、現在マスタとなっているノードのデータのみが表示されます。一方、*【ログおよびレポーティング(Logging & Reporting)】>>【ネットワーク使用状況(Network Usage)】*ページなどに表示されるアカウンティング情報には、関連するすべてのノードから収集されたデータが表示されます。たとえば、今日のCPU使用状況のヒストグラムには、マスタノードの現在のプロセッサ使用状況が表示されます。切り替わりが発生した場合、ここにはスレーブノードのデータが表示されるようになります。一方、上位アカウンティングサービスに関する情報などは、ユニットを通過するトラフィックの分散処理に関与したすべてのノードから収集されたデータの集合体となります。

注記

- *アドレス解決プロトコル*(ARP)を使用するのは、実際のマスタのみです。つまり、スレーブノードとワーカノードはARP要求の送信や応答を行いません。
- フェイルオーバーが発生すると、オペレーションを引き継ぐユニットがARPアナウンスメント(別名「*gratuitous ARP*」)を実行します。これは通常、要求を受信する他のホストのARPキャッシュを更新することを目的とするARP要求です。Gratuitous ARPは、マスタのIPがスレーブに移行したことをアナウンスするために使用されます。
- マスタで設定するすべてのインタフェースには物理リンクが必要です。つまり、任意のネットワークデバイスにポートを正しく接続しなければなりません。

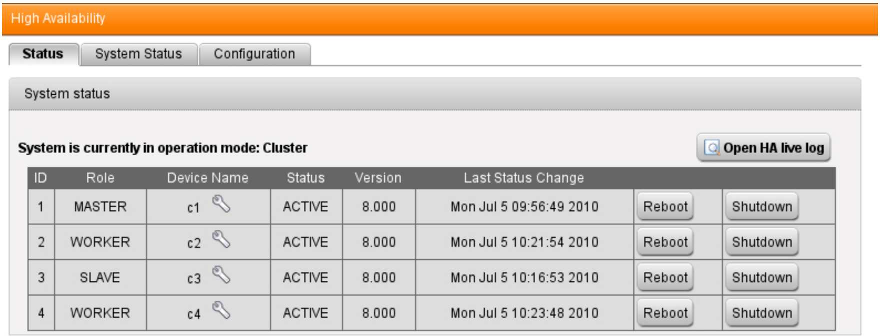
4.11.1 ハードウェアとソフトウェアの要件

HAフェイルオーバーまたはクラスタ機能を提供するためには、次のハードウェアおよびソフトウェア要件を満たす必要があります。

- 冗長化オプションが使用可能な有効なライセンス(スタンバイユニットの場合、追加の基本ライセンスのみが必要です)。
- ソフトウェアバージョンとハードウェアが同じである2台のASGユニット、または同じモデルの2台のASGアプライアンス。

- ハートビートが可能なイーサネットネットワークカード。サポートされているネットワークカードを確認するには、HCLをチェックしてください。HCLはAstaroナレッジベースで提供されています(検索用語に「HCL」を使用します)。
- イーサネットクロスオーバーケーブル(ホットスタンバイシステムでのマスタとスレーブの接続用)。ASG専用HAインタフェースがギガビット自動MDXデバイスであるアプライアンスのモデル320、425、525は、標準のIEEE 802.3イーサネットケーブルで接続可能です(イーサネットポートが送信/受信ペアを自動的に交換するため)。
- ネットワークスイッチ(クラスタノードの接続用)。

4.11.2ステータス



ID	Role	Device Name	Status	Version	Last Status Change		
1	MASTER	c1	ACTIVE	8.000	Mon Jul 5 09:56:49 2010	Reboot	Shutdown
2	WORKER	c2	ACTIVE	8.000	Mon Jul 5 10:21:54 2010	Reboot	Shutdown
3	SLAVE	c3	ACTIVE	8.000	Mon Jul 5 10:16:53 2010	Reboot	Shutdown
4	WORKER	c4	ACTIVE	8.000	Mon Jul 5 10:23:48 2010	Reboot	Shutdown

図30 冗長化(HA):【ステータス(Status)】ページ

*【マネジメント(Management)】>>【冗長化(High Availability)】>>【ステータス(Status)】*タブには、ホットスタンバイシステムまたはクラスタに関与するすべてのデバイスがリストされ、次の情報が表示されます。

- **ID**: デバイスのノードID。ホットスタンバイシステムでは、ノードIDは1(マスタ)または2(スレーブ)です。
  クラスタ内のノードIDは1～10の範囲になります。この理由は、1つのクラスタに最大10ノードまで持たせることができるためです。
- **役割(Role)**: クラスタ内の各ノードは次のいずれかの役割を果たすことができます。
  - マスタ(MASTER):ホットスタンバイ/クラスタセットアップ内のプライマリシステム。クラスタ内でデータの同期と配信を行う責任を担います。
  - スレーブ(SLAVE):ホットスタンバイ/クラスタセットアップ内のスタンバイシステム。マスタに障害が発生すると、オペレーションを引き継ぎます(テイクオーバーします)。
  - ワーカ(WORKER):データ処理のみを担当するシンプルなクラスタノード。

- **デバイス名(Device Name)**: デバイスの名前。
- **ステータス(Status)**: HAステータスに関するデバイスの状態。次のいずれかになります。
  - アクティブ(ACTIVE):ノードは完全に操作可能です。
  - リンク解除済み(UNLINKED):1つ以上のインタフェースリンクがダウンしています。
  - UP2DATE:Up2Dateが進行中です。
  - UP2DATE失敗(UP2DATE-FAILED):Up2Dateが失敗しました。
  - デッド(DEAD):ノードに到達できません。
  - 同期中(SYNCING):データ同期が進行中です。このステータスは、引き継ぎプロセスの進行中に表示されます。最初の同期には5分以上時間がかかります。あらゆる同期関連のプログラムにより、この時間が長期化する場合もあります。スレーブが同期中であり【*同期中(SYNCING)*】ステータスの場合、マスタノードでのリンク障害などが原因で正常な引き継ぎは行われません。
- **バージョン(Version)**: システムにインストールされたAstaro Security Gatewayソフトウェアのバージョン番号。
- **最後のステータス変化(Last Status Change)**: ステータス変更が最後に発生した時間。

リブート(Reboot)/シャットダウン(Shutdown): これらのボタンを使用して、デバイスを手動でリブートまたはシャットダウンすることができます。

ノード削除(Remove Node): このボタンを使用して、WebAdmin経由でデッド(Dead)状態のクラスタノードを削除します。メール隔離やスプールなど、ノード固有のすべてのデータがマスタに引き継がれます。

HAライブログを別ウィンドウで表示するには、右上隅にある【*HAライブログを開く(Open HA Live Log)*】ボタンをクリックします。

4.11.3システムステータス

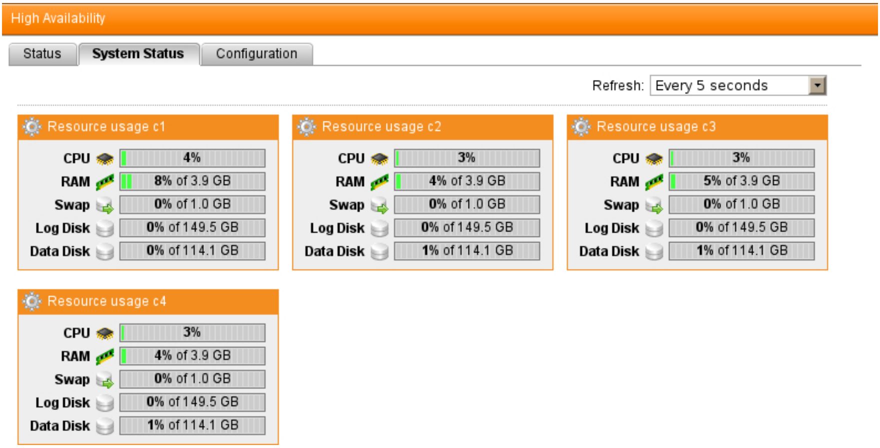


図31 冗長化:シングルHAまたはクラスタデバイスのリソース使用状況

*【マネジメント(Management)】>>【冗長化(High Availability)】>>【システムステータス(System Status)】*タブには、ホットスタンバイシステムまたはクラスタに関与するすべてのデバイスがリストされ、各デバイスのリソース使用状況に関する次の情報が表示されます。

- CPU使用状況(%)
- RAM使用状況
- スワップ使用状況(%)
- ログパーティションで消費されているハードディスクの容量(%)
- ルートパーティションで消費されているハードディスクの容量(%)

4.11.4設定

Astaro Security Gatewayの冗長化機能は、3つの基本設定をカバーします。

- 自動設定
- ホットスタンバイ(active-passive)
- クラスタ(active-active)

自動設定：Astaro Security Gateway には、ASGアプライアンス用のプラグアンドプレイ設定オプションがあります。このオプションを使用すると、クラスタに追加するデバイスを再設定したり手動でインストールしたりする必要なく、ホットスタンバイシステム/クラスタをセットアップすることができます。ASGアプライアンスの専用HAインタフェース(`eth3`)を相互接続し、すべてのデバイスで【*自動設定(Automatic Configuration)*】を選択するだけで、準備は完了です。

> **注 -** *自動設定*が正常に機能するためには、すべてのASGアプライアンスは同じモデルでなければなりません。たとえば、HAシステムのセットアップには、2台のASG 320アプライアンスを使用する必要があり、ASG 220ユニットとASG 320ユニットを組み合わせて使用することはできません。

この専用インタフェースを介して2台のASGアプライアンスを接続すると、すべてのデバイスが相互に認識し、HAシステムとして自動的に自己設定します。アップタイムが長い方のデバイスがマスタとなります。可能性は低いものの、アップタイムが同じであった場合には、MACアドレスに基づいてマスタとなるデバイスが決まります。

ASGソフトウェアを使用すると、専用スレーブシステムで【*自動設定(Automatic Configuration)*】オプションが使用され、マスタまたはすでに設定されているホットスタンバイシステム/クラスタに自動的に追加されます。このため、【*自動設定(Automatic Configuration)*】は、それ自体、高可用性オペレーションモードではなく移行モードと考えることができます。【*自動設定(Automatic Configuration)*】が選択されているデバイスがホットスタンバイシステムまたはクラスタに追加されると、高可用性オペレーションモードはそれぞれ【*ホットスタンバイ(Hot Standby)*】または【*クラスタ(Cluster)*】となります。ただし、この機能が正常に機能するためには、マスタシステムで【*自動追加(Autojoin)*】オプションが有効になっていることが条件となります。【*自動追加(Autojoin)*】機能により、高可用性オペレーションモードが【*自動設定(Automatic Configuration)*】に設定されているデバイスがホットスタンバイシステム/クラスタに自動的に追加されます。

ホットスタンバイ(active-passive)：Astaro Security Gateway では、2つのノードから成るホットスタンバイ高可用性コンセプトが採用されており、冗長性を実現する最低要件となります。Astaro Security GatewayソフトウェアV8に導入された主な改良点の1つに、テイクオーバー(引き継ぎ)のレイテンシを2秒未満に低減できる点があります。ファイアウォールは、ファイアウォール接続の同期化に加え、IPsecトンネルの同期化にも対応してます。つまり、ロードウォリアやリモートVPNゲートウェイが、テイクオーバー後にIPsecトンネルを再度確立する必要はありません。また、隔離されたオブジェクトも同期化されるため、テイクオーバー後も使用可能です。

クラスタ(active-active)： 大量のインターネットトラフィックのリアルタイム処理に対する需要が高まっています。これに対応するために、Astaro Security Gatewayには、処理集約型のタスク(コンテンツフィルタ、ウイルススキャン、侵入防止、復号化など)を複数のクラスタノードに均一に分

散するためのクラスタリング機能が用意されています。専用のハードウェアベースの負荷分散装置を使用する必要なく、ゲートウェイの全体的なパフォーマンスを大幅に向上できます。

注 - クラスタの設定時は、マスタノードを設定してから残りのユニットをスイッチに接続してください。

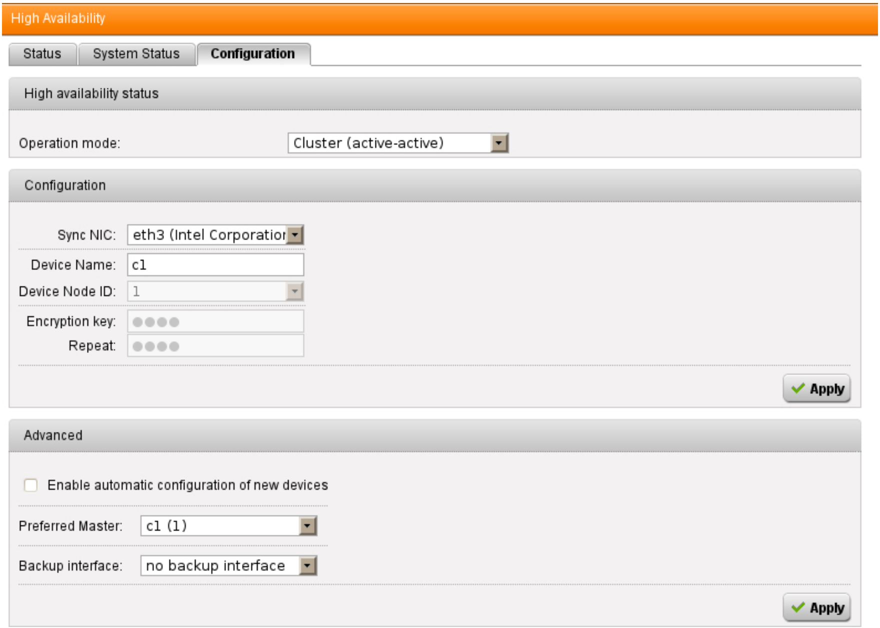


図32 冗長化:クラスタの設定

ホットスタンバイシステム/クラスタのマスタをセットアップするには、次の手順に従ってください。

1. **高可用性オペレーションモードを選択します。**
   デフォルトでは、高可用性はオフになっています。次のモードを使用できます。
   - 自動設定
   - ホットスタンバイ(active-passive)
   - クラスタ(active-active)

   【*ホットスタンバイ(Hot Standby)*】または【*クラスタ(Cluster)*】を選択します。

> **注 -** 高可用性オペレーションモードを変更する場合、モードを【*自動設定(Automatic Configuration)*】、【*ホットスタンバイ(Hot Standby)*】、または【*クラスタ(Cluster)*】に変更するためには、モードを一度【*オフ(Off)*】に戻す必要があります。

2. **次の設定を行います。**
   Sync NIC: マスタシステムとスレーブシステムとの通信で経由するネットワークインタフェースカードを選択します。リンクアグリゲーションがアクティブである場合、ここでリンクアグリゲーションインタフェースも選択できます。

   > **注 -** まだ設定していないインタフェースのみが表示されます。

   次のオプションは、オペレーションモードとして【*ホットスタンバイ(Hot Standby)*】または【*クラスタ(Cluster)*】を選択した場合のみ設定できます。

   デバイス名(Device Name): このデバイスを説明する名前を入力してください。

   デバイスノードID(Device Node ID): デバイスのノードIDを選択します。プライマリシステムに障害が発生した場合、IDが最も高いノードがマスタとなります。

   暗号鍵(Encryption Key): マスタとスレーブの通信を暗号化するパスフレーズ(確認のためにパスフレードを2回入力します)。鍵の最大長は16文字です。

3. **【*適用(Apply)*】をクリックします。**
   マスタで高可用性フェイルオーバーがアクティブになりました。

4. **オプションで、次の詳細設定を行います。**
   自動追加(Autojoin): ホットスタンバイシステム/クラスタを手動で設定した場合、【*自動追加(Autojoin)*】機能により、高可用性オペレーションモードが【*自動設定(Automatic Configuration)*】に設定されているデバイスがホットスタンバイシステム/クラスタに自動的に追加されます。

   > **注 -** HA同期化インタフェースに障害が発生した場合、設定はそれ以上同期されなくなります。バックアップインタフェースは、マスタ/マスタの状況を回避するだけです。

5. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

ここで、スレーブシステムのセットアップに進みます。

1. **高可用性オペレーションモードを選択します。**
   デフォルトでは、高可用性はオフになっています。

   次のモードを使用できます。

   - 自動設定
   - ホットスタンバイ(active-passive)
   - クラスタ(active-active)

   自動設定を選択した場合、マスタとの通信用のインタフェースのみを選択する必要があります。

2. **次の設定を行います。**
   Sync NIC: マスタシステムとスレーブシステムとの通信で経由するネットワークインタフェースカードを選択します。リンクアグリゲーションがアクティブである場合、ここでリンクアグリゲーションインタフェースも選択できます。次のオプションは、オペレーションモードとして【*ホットスタンバイ(Hot Standby)*】または【*クラスタ(Cluster)*】を選択した場合のみ設定できます。

   デバイス名(Device Name): このデバイスを説明する名前を入力してください。

   デバイスノードID(Device Node ID): デバイスのノードIDを選択します。プライマリシステムに障害が発生した場合、IDが最も高いノードがマスタとなります。

   暗号鍵(Encryption Key): マスタとスレーブの通信を暗号化するパスフレーズ(マスタで設定されているものと同じパスフレードを入力します)。鍵の最大長は16文字です。

3. ***【適用(Apply)】*をクリックします。**
   マスタで高可用性フェイルオーバーがアクティブになりました。

4. **オプションで、次の詳細設定を行います。**
   自動追加(Autojoin): ホットスタンバイシステム/クラスタを手動で設定した場合、【*自動追加(Autojoin)*】機能により、高可用性オペレーションモードが【*自動設定(Automatic Configuration)*】に設定されているデバイスがホットスタンバイシステム/クラスタに自動的に追加されます。ただし、このオプションはスレーブシステムに一切影響を与えないため、デフォルト設定のまま有効にしておくことができます。

   > **注 -** HA同期化インタフェースに障害が発生した場合、設定はそれ以上同期されなくなります。バックアップインタフェースは、マスタ/マスタの状況を回避するだけです。

5. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

ホットスタンバイモードのゲートウェイは、データ転送接続に対して定期的に更新されます。アクティブなプライマリシステムでエラーが発生した場合、速やかにセカンダリシステムが通常モードに自動的に切り替わり、プライマリシステムの機能を引き継ぎます。

注 - ホットスタンバイシステム/クラスタを無効にすると、スレーブノードとワーカノードは工場出荷時の状態に戻り、シャットダウンします。

詳細情報(特に使用事例)は、Astaroナレッジベースにある『*HA/クラスタガイド(HA/Cluster Guide)*』で確認できます。

設定

実行中の設定で同期化インタフェースを変更することができます。その後、すべてのノードはリブートします。

詳細

このセクションでは、詳細設定を行うことができます。

新しいデバイスの自動設定を有効化(Enable Automatic Configuration of New Devices): このオプションはデフォルトでアクティブになっており、新たに接続されたデバイスは自動的に設定されます。

優先マスタ(Preferred Master): ここでは、ドロップダウンリストでノードを選択して、指定のマスタノードを定義できます。フェイルオーバーが発生した場合、選択されたノードはリンクの回復後はスレーブモードのままではなく、マスタモードにスイッチバックします。

バックアップインタフェース(Backup Interface): HA同期化インタフェースの障害やネットワークケーブルの切断などが原因で、マスタとスレーブの両方が同時にマスタになること(マスタ/マスタの状況)を防ぐために、バックアップ用のハートビートインタフェースを選択できます。この追加ハートビートインタフェースには、いずれかの設定済みアクティブイーサネットインタフェースを選択できます。バックアップインタフェースを選択すると、マスタ/スレーブ設定が維持されていることを確認するために、このインタフェース経由で追加のハートビート信号が一方向へ(マスタからスレーブへ)送信されます。マスタ/スレーブ接続が無効であり、バックアップインタフェースが関与すると、いずれかのクラスタノードが停止していることを知らせる通知が管理者に送信されます。ただし、このオプションはスレーブシステムに一切影響を与えないため、未設定のままにしておくことができます。

4.12シャットダウンとリスタート

このタブでは、手動でシャットダウンまたはリスタートできます。Astaro Security Gateway.

シャットダウン(Shutdown): この操作により、システムをシャットダウンして、すべてのサービスを適切に停止できます。モニタやLCDディスプレイが接続されていないシステムの場合は、シャットダウンプロセスの最後にビープ音が1秒間隔で鳴り続けます。

シャットダウンするには、Astaro Security Gateway以下の手順に従います。

1. ***【システムをシャットダウン(停止)(Shutdown (Halt) the System Now)】をクリックします。***
2. **警告メッセージを確認します。**
   【システムをシャットダウンしますか?(Really shut down the system?)】というメッセージが表示されたら、*【OK】*をクリックします。

   システムはシャットダウンして停止します。

お使いのハードウェアおよび設定により、シャットダウンが完了するまでに数分かかる場合があります。システムが完全にシャットダウンした後で、電源を切ります。システムが完全にシャットダウンする前に電源を切ると、システムが次回の起動(ブート)時にファイルシステムの一貫性をチェックするため、起動プロセスに通常よりかなり長く時間がかかることになります。最悪の場合は、データが失われる場合があります。

システムの起動が正常に行われるとビープ音が連続して5回鳴ります。

リスタート: この操作により、システムを完全にシャットダウンして再起動(リブート)します。お使いのハードウェアおよび設定により、完全にリスタートするまでに数分かかる場合があります。

リスタートするには、Astaro Security Gateway以下の手順に従います。

1. ***【システムをリスタート(リブート)(Restart (Reboot) the System Now)】をクリックします。***
2. **警告メッセージを確認します。**
   【システムをリスタートしますか?(Really restart the system?)】というメッセージが表示されたら、*【OK】*をクリックします。

   システムはシャットダウンし、停止してからリブートします。

5定義およびユーザ

この章では、Astaro Security Gateway全体で使用されるネットワーク、サービス、期間の定義を設定する方法について説明します。WebAdminの【*オブジェクト定義の概要(Definitions Overview)*】ページは、タイプに基づくネットワーク定義の数と、プロトコルタイプに基づくサービス定義の数を示します。

【*定義およびユーザ(Definitions & Users)*】メニューのページを使用すると、他のすべての設定メニューで使用できるネットワークとサービスを一元的に定義することができます。これにより、IPアドレス、ポート、ネットワークマスクなどに悩まされることなく、名前を使用して作業できます。その他のメリットとしては、個々のネットワークやサービスをグループにまとめて、一度に設定できることがあげられます。後でこれらのグループに特定の設定を割り当てたりすると、これらの設定はグループに含まれるすべてのネットワークとサービスに適用されます。

さらに、この章では、Astaro Security Gatewayのユーザアカウント、ユーザグループ、および外部認証サーバの設定方法や、クライアントPCの認証について説明します。

この章には次のトピックが含まれます。

- ネットワーク定義
- サービス定義
- 期間定義
- ユーザ&グループ
- クライアント認証
- 認証サーバ

5.1 ネットワーク定義

【*定義およびユーザ(Definitions & Users)*】>>【*ネットワーク定義(Network Definitions)*】ページは、ASGのホスト、ネットワーク、ネットワークグループを一元的に定義する場所です。ここで作成した定義は、他の多くのWebAdmin設定メニューでも使用できます。

ヒント - *ネットワーク定義*リストでネットワーク定義の情報アイコンをクリックすると、ネットワーク定義が使用されるすべての設定オプションを表示できます。

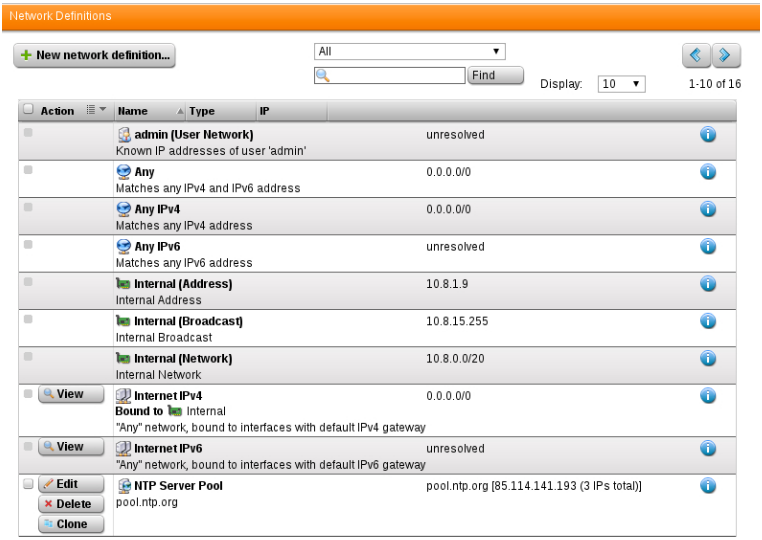


図33 定義(Definitions):ネットワーク定義のリスト

ネットワークテーブルには、システムが自動的に作成した、編集も削除もできない静的ネットワークも含まれています。

- **インタフェースアドレス(Interface Address)**: このタイプの定義は、各ネットワークインタフェースに追加されます。ここには、インタフェースの現在のIPアドレスが含まれています。名前では、インタフェース名の後に「(Address)」という言葉が付いています。
- **インタフェースブロードキャストアドレス(Interface Broadcast Address)**: このタイプの定義は、各イーサネットタイプネットワークインタフェースに追加されます。ここには、インタフェースの現在のIPv4ブロードキャストアドレスが含まれています。名前では、インタフェース名の後に「(Broadcast)」という言葉が付いています。
- **インタフェースネットワークアドレス(Interface Network Address)**: このタイプの定義は、各イーサネットタイプネットワークインタフェースに追加されます。ここには、インタフェースの現在のIPv4ネットワークが含まれています。名前では、インタフェース名の後に「(Network)」という言葉が付いています。
- **インターネット(Internet)**: インタフェースに関連付けられたネットワーク定義。デフォルトゲートウェイとして機能します。設定でこれを使用すると、設定プロセスが容易になります。【*アップリンクバランシング(Uplink Balancing)*】を有効にすると、*インターネットはアップリンクインタフェースと関連付けられます*。

ネットワーク定義を作成するには、次の手順に従います。

1. ***【ネットワーク定義(Network Definitions)】ページで【新規ネットワーク定義(New Network Definition)】をクリックします。***
   *【新規ネットワーク定義の作成(Create New Network Definition)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   (選択した定義タイプに応じて、ネットワーク定義のさらに詳細なパラメータが表示されます。)

   名前(Name): この定義を説明する名前を入力します。

   タイプ(Type): ネットワーク定義タイプを選択します。次のタイプを使用できます。

   - **ホスト(Host)**: 1つのIPv4アドレス。次の情報を指定します。
     - **アドレス(Address)**: ホストのIPアドレス(設定されたインタフェースのIPアドレスを入力することはできません)。
     - **インタフェース(Interface)**(オプション):ネットワーク定義を特定インタフェースにバインドして、その定義への接続がこのインタフェース経由でのみ確立されるようにすることができます。
     - **コメント(Comment)**(オプション):説明などの情報を追加します。
   - **DNSホスト(DNS Host)**:DNSホスト名。システムによって動的に解決され、IPアドレスが生成されます。DNSホストは、動的IPエンドポイントの使用時に便利です。システムは、TTL(生存時間)の値に従って定期的にこれらの定義を再解決し、新しいIPアドレスがある場合は定義を更新します。次の情報を指定します。
     - **インタフェース(Interface)**(オプション):ネットワーク定義を特定インタフェースにバインドして、その定義への接続がこのインタフェース経由でのみ確立されるようにすることができます。
     - **ホスト名(Hostname)**: 解決したいホスト名。
     - **コメント(Comment)**(オプション):説明などの情報を追加します。
   - **DNSグループ(DNS Group)**: DNSホストと似ていますが、1つのホスト名用のDNS内の複数のRR(リソースレコード)を処理できます。透過プロキシでのファイアウォールルールと例外の定義に便利です。
   - **ネットワーク(Network)**: 標準的なIPv4ネットワーク。ネットワークアドレスとネットマスクから構成されています。次の情報を指定します。
     - **アドレス(Address)**: ネットワークのネットワークアドレス(設定されたインタフェースのIPアドレスを入力することはできません)。

  - **インタフェース(Interface)**(オプション):ネットワーク定義を特定インタフェースにバインドして、その定義への接続がこのインタフェース経由でのみ確立されるようにすることができます。
  - **ネットマスク(Netmask)**: オクテット内のいくつのビットでサブネットワークが指定され、いくつのビットがホストアドレスに使用されるかを示すために使用されるビットマスク。
  - **コメント(Comment)**(オプション):説明などの情報を追加します。
- **マルチキャストグループ(Multicast Group)**: 定義されたマルチキャストネットワーク範囲から構成されるネットワーク。
  - **アドレス(Address)**: マルチキャストネットワークのネットワークアドレス。`224.0.0.0`〜`239.255.255.255`の範囲である必要があります。
  - **インタフェース(Interface)**(オプション):ネットワーク定義を特定インタフェースにバインドして、その定義への接続がこのインタフェース経由でのみ確立されるようにすることができます。
  - **ネットマスク(Netmask)**: オクテット内のいくつのビットでサブネットワークが指定され、いくつのビットがホストアドレスに使用されるかを示すために使用されるビットマスク。
  - **コメント(Comment)**(オプション):説明などの情報を追加します。
- **ネットワークグループ(Network Group)**: 他のネットワーク定義のリストが含まれるコンテナ。これらを使用してネットワークとホストをバンドルすると、設定がより読みやすくなります。*ネットワークグループ*を選択すると、【*メンバ(Members)*】ボックスが表示され、グループメンバを追加できます。
- **可用性グループ(Availability Group)**: ホストまたはDNSホスト(あるいはその両方)のグループ。優先順位に基づいてソートされています。ICMP pingにより、すべてのホストの生存ステータスが指定の間隔でチェックされます。優先順位が最も高く、生存ステータスであるホストが設定で使用されます。
  - **メンバ(Members)**: グループメンバを追加します。
  - **チェック間隔(Check Interval)**: ホストをpingチェックする間隔を秒単位で入力します。
  - **常に解決(Always Resolved)**: このオプションはデフォルトで選択されているため、すべてのホストが使用不可である場合、グループは最後に使用可能であったホストで解決されます。これを選択しないと、グループは*未解決*に設定されます。

3. **【保存(Save)】をクリックします。**
   新しい定義がネットワーク定義リストに表示されます。

ネットワーク定義を編集または削除するには、対応するボタンをクリックします。

5.2サービス定義

*【定義およびユーザ(Definitions & Users)】>>【サービス定義(Service Definitions)】*ページで、サービスおよびサービスグループを定義して一元管理できます。サービスは、特定タイプのネットワークトラフィックの定義で、TCP、またはUDPといったプロトコルに関する情報とプロトコル関連オプション(ポート番号など)に関する情報を組み合わせています。サービスを使用して、ゲートウェイで許可または定義されるトラフィックのタイプを決定することができます。

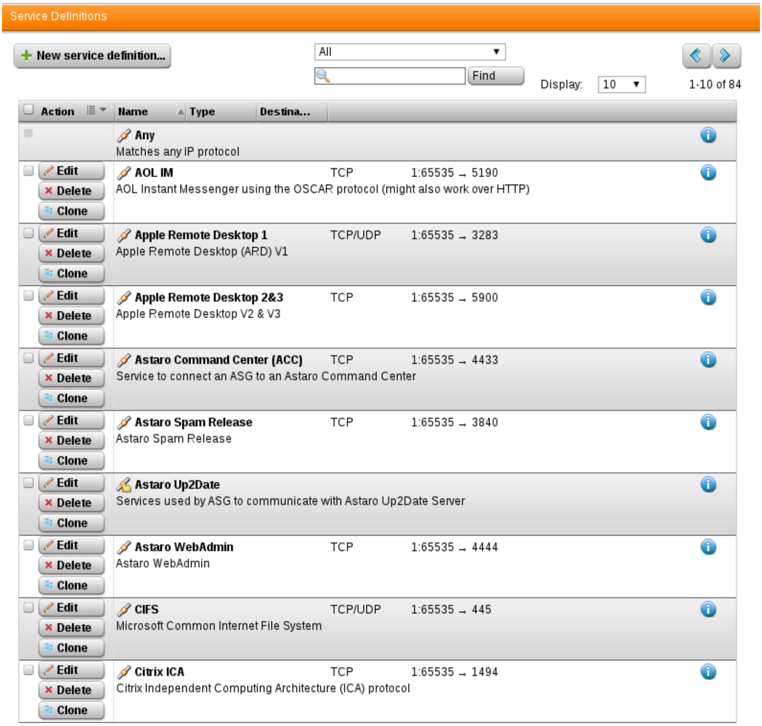


図34 定義(Definitions):サービス定義リスト

ヒント -【*サービス定義(Service Definitions)*】リストのサービス定義の情報アイコンをクリックすると、サービス定義が使用されているすべての設定オプションを表示できます。

サービス定義を作成するには、以下の手順に従います。

1. **【サービス定義(Service Definitions)】ページで【新規サービス定義(New Service Definition)】をクリックします。**
   【*新規サービス定義の作成(Create New Service Definition)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   (選択した定義タイプに応じて、ネットワーク定義のさらに詳細なパラメータが表示されます。)

   名前(Name): この定義を説明する名前を入力します。

   定義タイプ(Type of Definition): サービスタイプを選択します。次のタイプを使用できます。

   - **TCP**: TCP(伝送制御プロトコル)接続では、0〜65535のポート番号を使用します。ロストしたパケットはTCPが認識して再度リクエストします。TCP接続では、受信者は送信者に対してデータパケットを受信したときに通知します(接続関連のプロトコル)。TCPセッションは3WAYハンドシェークで始まり、セッションの最後に接続がクローズします。次の情報を指定します。
     - **宛先ポート(Destination Port)**: 宛先ポートを単一のポート番号(例:80)あるいは範囲(例:1024:64000)として入力します。範囲を指定する場合は、コロンを区切り文字として使用します。
     - **送信元ポート(Source Port)**: 送信元ポートを単一のポート番号(例:80)あるいは範囲(例:1024:64000)として入力します。範囲を指定する場合は、コロンを区切り文字として使用します。
   - **UDP**:*UDP(User Datagram Protocol)*は、0〜65535のポート番号を使用するステートレスプロトコルです。UDPはステートを維持しないため、TCPより高速です。特に、少量のデータは高速に送信できます。ただし、このステートレスは、UDPはパケットがロストまたはドロップした場合に認識できないことも意味します。受信コンピュータは、データパケットを受信しても送信者に通知しません。*UDP*を選択した場合は、TCPの場合と同じ設定オプションを編集できます。

- **TCP/UDP**: TCPとUDPの組み合わせで、DNSなどの両方のサブプロトコルを使用するアプリケーションプロトコルに適切です。*TCP/UDP*を選択した場合は、TCPまたはUDPの場合と同じ設定オプションを編集できます。
- **ICMP/ICMPv6**:ICMP(*Internet Control Message Protocol*)は主にエラーメッセージの送信に使用されます。たとえば、要求されたサービスが利用できない、あるいはホストやルータに到達できなかった、などのメッセージを送信します。*ICMP*または*ICMPv6*を選択した場合は、ICMPコード/タイプを選択します。IPv4ファイアウォールルールはICMPv6では機能せず、IPv6ファイアウォールルールはICMPでは機能しません。
- **IP**:IP(*Internet Protocol*)は、インターネット上でのデータのやり取りに使用されるネットワークおよび伝送プロトコルです。*IP*を選択したら、IP内でカプセル化されるプロトコルの番号を指定します(例:`121`、これはSMPプロトコルを表します)。
- **ESP**:ESP(*カプセル化セキュリティペイロード*)は、IPsecトンネリングプロトコルスイートの一部で、VPNを介してトンネルされるデータに暗号化サービスを提供します。ESPまたはAHを選択した場合は、*SPI(セキュリティパラメータインデックス)*を指定します。これは、IPアドレスとともにセキュリティパラメータを特定します。特に自動IPsec鍵交換を使用する場合は、256～4,294,967,296の値を入力するか、または256～4,294,967,296の範囲として指定されたデフォルト設定を使用します(コロンを区切り文字として使用します)。1～255の番号は*IANA(Internet Assigned Numbers Authority)*によって予約されています。
- **AH**:*認証*ヘッダー(AH)はIPsecトンネリングプロトコルスイートの一部で、IPヘッダとデータグラムペイロード間に位置し、情報の(機密性ではなく)整合性を維持します。
- **グループ(Group)**: その他のサービス定義リストを含むコンテナ。設定を読みやすくするために、これらを使用してサービス定義をまとめることができます。*【グループ(Group)】*を選択すると、*【メンバ(Members)】*ダイアログボックスが開くので、そこでグループのメンバ(その他のサービス定義)を追加します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しい定義がサービス定義リストに表示されます。

定義を編集または削除するには、対応するボタンをクリックします。

> **注 -**定義タイプは後で変更できません。定義タイプを変更するには、サービス定義を削除し、希望の設定で新しいサービス定義を作成します。

5.3期間定義

*【定義およびユーザ(Definitions & Users)】>>【期間定義(Time Period Definitions)】*ページで、単独または繰り返し発生する時間帯(タイムスロット)を定義できます。これを使用して、コンテンツフィルタプロファイルの割り当てを特定の時間範囲に制限できます。

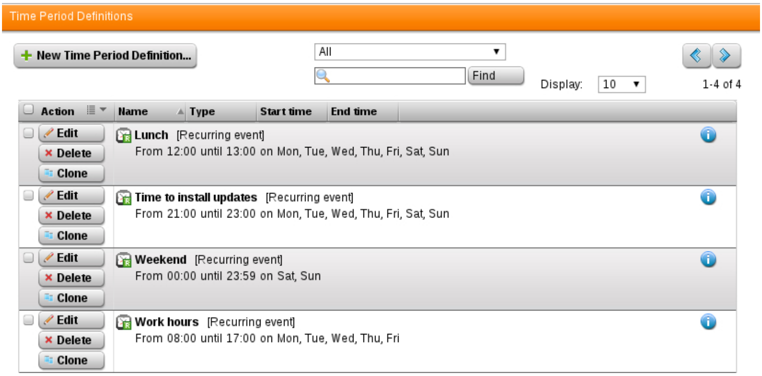


図35 定義(Definitions):タイムイベント定義リスト

ヒント -*【期間定義(Time Period Definitions)】*リストの期間定義の情報アイコンをクリックすると、その期間定義が使用されているすべての設定オプションを表示できます。

期間定義を作成するには、以下の手順に従います。

1. ***【期間定義(Time Period Definitions)】*タブで*【新規期間定義(New Time Period Definition)】*をクリックします。**
   *【新規期間定義を作成(Create New Time Period Definition)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): この期間定義を説明する名前を入力します。

   タイプ(Type): 期間定義のタイプを選択します。次のタイプを使用できます。

   - **繰り返しイベント(Recurring Event)**: これらのイベントは定期的に繰り返されます。開始時間、終了時間、および期間定義が適用される曜日を選択できます。このタイプには開始日と終了日は選択できません。

- **単独のイベント(Single Event)**: これらのイベントは一度だけ実施されます。開始日時および終了日時の両方を選択できます。これらの定義は繰り返されないので、【*曜日(Weekdays)*】オプションはこのタイプには選択できません。
- **コメント(Comment)**(オプション): 説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
   新しい期間定義が【*期間定義(Time Period Definitions)*】リストに表示されます。

期間定義を編集あるいは削除するには、該当するボタンをクリックします。

> **注 -** ファイアウォールルールまたはフィルタ割り当て内で使用されていない期間定義のみを削除できます。

5.4ユーザ&グループ

【*定義およびユーザ(Definitions & Users)*】>>【*ユーザとグループ*】*Users & Groups)*】メニューを使用して、WebAdminアクセス、リモートアクセス、ユーザポータルアクセス、Eメールの使用のためのユーザとグループを作成することができます。

5.4.1ユーザ

【*定義およびユーザ(Definitions & Users)*】>>【*ユーザとグループ(Users & Groups)*】>>【*ユーザ(Users)*】タブで、ゲートウェイにユーザアカウントを追加することができます。工場出荷時のデフォルト設定では、Astaro Security Gateway には*admin*という1人の管理者が構成されています。

> **ヒント -**【*ユーザ(Users)*】リストのユーザ定義の情報アイコンをクリックすると、ユーザ定義が使用されているすべての設定オプションを表示できます。

【*新規ユーザ(New User)*】ダイアログボックスでEメールアドレスを指定すると、このユーザのX.509証明書が生成されるのと同時に、Eメールアドレスを証明書のVPNIDとして使用してユーザ定義が作成されます。Eメールアドレスが指定されていない場合は、ユーザの*識別名*(DN)をVPN IDとして証明書が作成されます。このように、ユーザがeDirectoryなどのバックエンドグループにより認証されている場合は、対応するバックエンドユーザオブジェクトでEメールアドレスが設定されていない場合でも証明書は作成されます。

なぜなら、各証明書のVPN IDは一意であるため、各ユーザ定義は異なる一意のEメールアドレスを使用しているからです。システムにすでにあるEメールアドレスを使用したユーザ定義の作成は失敗します。証明書は、Astaro Security Gatewayがサポートする各種リモートアクセス方法で使用可能です。ただし、PPTP、PSKを使用するL2TP over IPsec、およびRSAまたはPSKを使用するネイティブIPsecは除外されます。

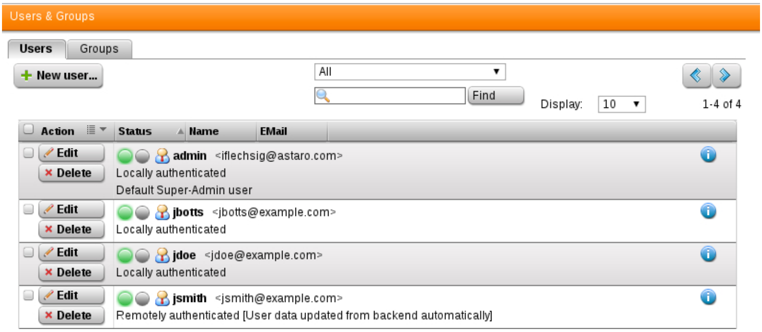


図36 ユーザ(Users):ユーザリスト

ユーザアカウントを追加するには、以下の手順に従います。

1. ***【ユーザ(Users)】タブで、【新規ユーザ(New User)】をクリックします。***
   *【新規ユーザの作成(Create New User)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ユーザ名(Username): このユーザを説明する名前を入力します(例:jdoe)。

   実際の名前(Real Name): ユーザの実際の名前を入力します(例:John Doe)。

   Eメールアドレス(E-mail Address): ユーザのプライマリEメールアドレスを入力します。

   他のEメールアドレス(Additional E-mail Addresses)(オプション):このユーザの他のEメールアドレスを入力します。これらのEメールアドレスに送信されたスパムメールは各Eメールアドレス用の個々の隔離レポートにリストされ、このレポートは前述のプライマリEメールアドレスに送信されます。

   認証(Authentication): 認証方式を選択します。以下の方式を使用できます。

   - **ローカル(Local)**: この方式は、ゲートウェイ.
   - **リモート(Remote)**: 当製品でサポートされている外部認証方式のいずれかを使用してユーザを認証する場合に選択します。Astaro Security Gateway. 詳細は、*【定義およびユーザ(Definitions & Users)】>>【認証サーバ(Authentication Servers)】*を参照してください。

- **なし(None)**: ユーザが認証されるのを完全に防止する場合に選択します。これは、たとえば、ユーザ定義を削除することなくユーザを一時的に無効にする場合に役に立ちます。

パスワード(Password): ユーザのパスワードを入力します(確認のために2回入力します)。認証方式として【*ローカル(Local)*】を選択した場合のみ利用できます。基本的なユーザ認証ではウムラウトはサポートしていません。

バンクエンドの同期(Backend Sync): 実際の名前やユーザのEメールアドレスなどのユーザ定義の基本設定の一部を、データを外部バックエンド認証サーバと同期することで自動的に更新できます(認証方式として【*リモート(Remote)*】を選択したときのみ利用できます)。

注 - 現在は、Active DirectoryおよびeDirectoryサーバのデータのみ同期できます。

X.509証明書(X.509 Certificate): ユーザ定義を作成したら、ユーザ定義を編集する際にこのユーザにX.509証明書を割り当てることができます。デフォルトでは、この証明書はユーザ定義を作成したときに自動的に生成されたものです。ただし、サードパーティの証明書を割り当てることもできます。証明書は、【*リモートアクセス(Remote Access)*】>>【*証明書管理(Certificate Management)*】>>【*証明書(Certificates)*】タブでアップロードできます。

スタティックリモートアクセスIPを使用(Use Static Remote Access IP)(オプション):リモートアクセスを取得するユーザに、IPアドレスプールのダイナミックIPアドレスを割り当てる代わりにスタティックIPアドレスを割り当てる場合に選択します。NATルータ背後のIPsecユーザは、スタティックリモートアクセスIPアドレスを必ず使用する必要があります。

注 - スタティックリモートアクセスIPは、PPTP、L2TP、およびIPsecを介したリモートアクセスのみに使用できます。これは、SSLを介したリモートアクセスには使用できません。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **オプションで詳細設定を行います。**
   ユーザは独自のEメールホワイトリストとブラックリストを作成し、管理することができます(「ユーザポータル」の章を参照)。ここでこれらのリストを参照し、必要に応じて変更することができます。

4. **【*保存(Save)*】をクリックします。**
   新しいユーザアカウントが【*ユーザ(Users)*】リストに表示されます。

このユーザをWebベースの管理インタフェースWebAdminへのアクセスをもつ正規の管理者にする場合は、そのユーザを*SuperAdmins*グループに追加します。SuperAdminsは、WebAdminの*【定義およびユーザ(Definitions & Users)】>>【ユーザとグループ(Users & Groups)】>>【グループ(Groups)】*タブで設定します。

注 - ユーザオブジェクトを削除した後で同じ名前でユーザオブジェクトを作成する場合は、このユーザに関連する証明書も*【リモートアクセス(Remote Access)】>>【証明書管理(Certificate Management)】>>【証明書(Certificates)】*タブで削除したことを確認してください。削除していない場合、「その名前のアイテムはすでに存在します」という旨のエラーメッセージが表示されます。

5.4.2グループ

*【定義およびユーザ(Definitions & Users)】>>【ユーザとグループ(Users & Groups)】>>【グループ(Groups)】*ページで、ゲートウェイにユーザグループを追加することができます。工場出荷時のデフォルト設定として、Astaro Security Gatewayには*SuperAdmins*というユーザグループがあります。管理特権をユーザに割り当てたい(つまりWebAdminへのアクセス権をユーザに付与したい)場合は、当該ユーザを*SuperAdmins*グループに追加します。このグループは削除しないでください。

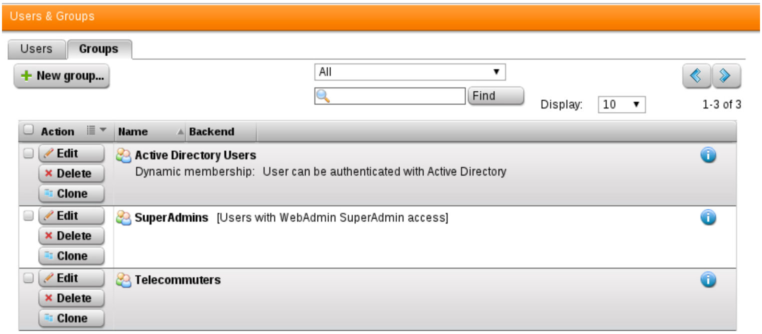


図37 グループ:グループのリスト

ヒント - *【グループ(Groups)】*リストでグループの定義をクリックすると、そのグループ定義が使用されているすべての設定オプションが表示されます。

ユーザグループを追加するには、次の手順に従ってください。

1. **【*グループ(Groups)*】タブで、【*新規グループ(New Group)*】をクリックします。**
   【*新規グループの作成(Create New Group)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   グループ名(Group Name): このグループを説明する名前を入力します。この名前は、バックエンドグループの名前に対応している必要はありません。

   グループタイプ(Group Type): グループのタイプを選択します。静的メンバのグループか、動的メンバシップを実現する2種類のグループタイプから選択できます。

   - **静的メンバ(Static Members)**: このグループのメンバとなるローカルユーザを選択します。
   - **IPsec X509 DNマスク(IPsec X509 DN Mask)**: ユーザは、IPsec接続によってゲートウェイへのログインに成功し、識別名に含まれる特定のパラメータが【*DNマスク(DN Mask)*】ボックスで指定された値と一致した場合に、IPsec X509 DNグループ定義に動的に追加されます。
   - **バックエンドメンバシップ(Backend Membership)**: ユーザは、サポートされるいずれかの認証メカニズムによる認証が成功した場合に、グループ定義に動的に追加されます。続行するには、該当するバックエンド認証タイプを選択します。
     - **Active Directory**: ゲートウェイのActive Directorユーザグループは、Windowsネットワーク上で設定されているActive Directoryサーバユーザグループのメンバに対し、グループメンバシップを提供します。このユーザがメンバとなっているActive Directoryサーバグループの名前を入力してください。詳細は、「*定義およびユーザ*」>>「*認証サーバ*」>>「*サーバ*」を参照してください。
     - **eDirectory**: ゲートウェイのeDirectoryユーザグループは、eDirectoryネットワーク上で設定されているeDirectoryユーザグループのメンバに対し、グループメンバシップを提供します。このユーザがメンバとなっているeDirectoryグループの名前を入力してください。詳細は、「*定義およびユーザ*」>>「*認証サーバ*」>>「*サーバ*」を参照してください。
     - **RADIUS**: ユーザは、RADIUS認証方式による認証が成功すると、RADIUSバックエンドグループに自動的に追加されます。
     - **TACACS+**: ユーザは、TACACS+認証方式による認証が成功すると、TACACS+バックエンドグループに自動的に追加されます。
     - **LDAP**: ユーザは、LDAP認証方式による認証が成功すると、LDAPバックエンドグループに自動的に追加されます。

バックエンドグループメンバシップに制限(Limit to Backend Group(s) Membership)(オプション):選択したバックエンドサーバのすべてのユーザをこのグループ定義に含めることを望まない場合は、すべてのX.500ベースのディレクトリサービスに対して、バックエンドサーバ上のいくつかのグループにメンバシップを制限することができます。このオプションを選択する場合、ここで入力するグループは、バックエンドサーバに設定されている一*般名*と一致している必要があります。Active Directoryバックエンドに対してこのオプションを選択する場合、`CN=`プレフィックスは省略できます。eDirectoryバックエンドに対してこのオプションを選択すると、eDirectoryブラウザを使用して、このグループ定義に含めるeDirectoryグループを簡単に選択することができます。ただし、eDirectoryブラウザを使用しない場合は、eDirectoryコンテナの入力時に`CN=`プレフィックスを必ず含めてください。

LDAP属性のチェック(Check an LDAP Attribute)(オプション):選択したバックエンドLDAPサーバのすべてのユーザをこのグループ定義に含めたくはない場合は、このチェックボックスにチェックを入れて、バックエンドサーバ上にある特定のLDAP属性に一致するユーザのみにメンバシップを制限することができます。この属性はLDAP検索フィルタとして使用されます。たとえば、属性として`groupMembership`を入力し、その値として`CN=Sales,O=Example`を入力することができます。これにより、会社の営業部門に属するすべてのユーザをグループ定義に含めることができます。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
新しいユーザグループが*【グループ(Groups)】*リストに表示されます。

グループを編集または削除するには、対応するボタンをクリックします。

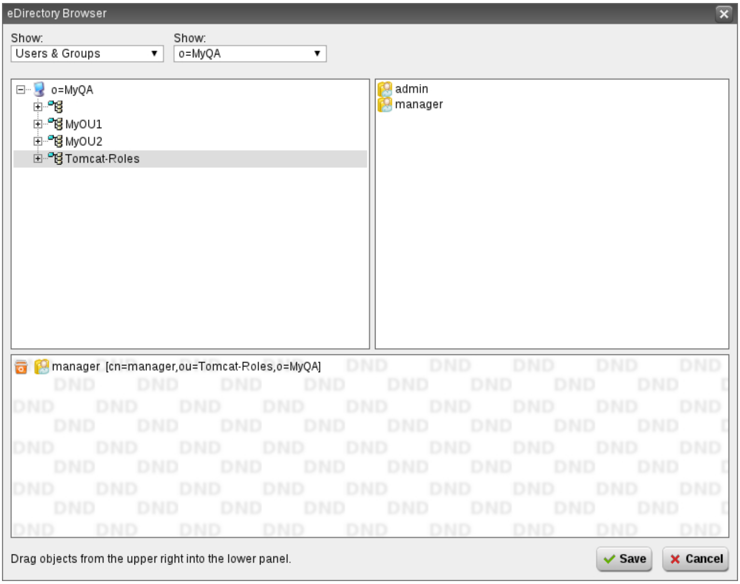


図 38 グループ(Groups):eDirectoryブラウザ - Astaro Security Gateway

5.5 クライアント認証

Astaroは、ユーザ認証をASGで直接認証を行うために、Windows用の認証クライアントを提供しています。これにより、ユーザネットワークまたはグループネットワークに基づくファイアウォールルールを作成したりすることで、Webサーフィンやネットワークトラフィックをユーザに基づいてコントロールすることができます。さらに、可能であれば、IPアドレス、ホスト名、その他の情報をユーザ名に置き換えるため、データやオブジェクトのレポートがより読みやすくなります。

クライアント認証を使用したい(あるいは使用する必要がある)ユーザは、クライアントPCにAstaro Authentication Agent(AAA)をインストールする必要があります。AAAは、このWebAdminページまたはユーザポータルからダウンロード可能です。ユーザポータルのページにダウンロードリンクが表示されるのは、クライアント認証設定のユーザグループに参加しているユーザのみです。

クライアント認証を設定するには、次の手順に従ってください。

1. ***【クライアント認証(Client Authentication)】タブで、クライアント認証を有効にします。***
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

ステータスアイコンが緑色になり、*【クライアント認証オプション(Client Authentication Options)】*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   クライアント認証を使用する必要があるネットワークを選択します。クライアント認証が機能するためには、これらのネットワークがASGに直接接続されている必要があります。

3. **許可するユーザおよびグループを選択します。**
   単一のユーザおよびグループを*【許可されるユーザおよびグループ(Allowed Users and Groups)】*ボックスで選択または追加します。これは、既存の認証グループ(Active Directoryユーザグループなど)にすることもできます。

4. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

   選択したネットワークでクライアント認証を利用できるようになりました。

クライアント認証プログラム

クライアント認証を有効にすると、ここでAstaro Authentication Agent(AAA)をダウンロードできます。AAAを手動で配布することも、ユーザがユーザポータルからダウンロードできるようにすることもできます。

AAAはWebフィルタの認証モードとして使用できます。詳しくは、「*Webセキュリティ*」>>「*Webフィルタ*」>>「*グローバル*」の章を参照してください。

5.6認証サーバ

【定義(Definitions)】&*【ユーザ(Users)】*>>*【認証サーバ(Authentication Servers)】*ページでは、外部ユーザ認証サービスのデータベースおよびバックエンドサーバを管理できます。外部ユーザ認証を使用すると、ネットワーク内の他のサーバ上にある既存のユーザデータベースやディレクトリサービスに対して、ユーザアカウントを検証することができます。現在サポートされている認証サービスは次のとおりです。

- NovellのeDirectory
- マイクロソフトのActive Directory
- RADIUS
- TACACS+
- LDAP

5.6.1グローバル設定

*【定義(Definitions)】&【ユーザ(Users)】>>【認証サーバ(Authentication Servers)】>>【グローバル設定(Global Settings)】*タブでは、基本的な認証オプションを設定できます。次のオプションを使用できます。

自動的にユーザを作成(Create Users Automatically): このオプションを選択した場合、設定済みのバックエンドグループの不明ユーザが、Astaro Security Gatewayでサポートされている各種認証サービスのいずれかに対する認証に成功すると、Astaro Security Gatewayは常にユーザオブジェクトを自動的に作成します。たとえば、RADIUSバックエンドグループを設定しており、*【マネジメント(Management)】>>【WebAdmin設定(WebAdmin Settings)】>>【アクセスコントロール(Access Control)】*タブの*【許可される監査役(Allowed Auditors)】*ボックスでこのグループを選択している場合、Astaro Security GatewayはWebAdminへのログインに成功したRADIUSユーザに対してユーザ定義を自動的に作成します。

- **機能別自動ユーザ作成(Automatic User Creation for Facilities)**: 自動ユーザ作成は、特定のサービスに対して有効または無効にすることができます。有効なサービスに対してのみ、ユーザが作成されます。*【自動的にユーザを作成(Create Users Automatically)】*オプションからチェックを外すと、このオプションは使用できず、ユーザの自動作成機能はすべてのファシリティに対して無効になります。

> **注 -** この機能は、Active Directoryの*シングルサインオン*(SSO)では機能しません。

これらのユーザオブジェクトは、Astaro Security Gatewayのユーザポータルへのアクセス権を付与するためにも必要です。さらに、自動作成されたすべてのユーザオブジェクトのために、SSL証明書が生成されます。ただし、Eメールアドレスが衝突する場合は、このユーザの自動作成は失敗します。この理由は、自動的に作成されるユーザ定義において、システムにすでに存在するEメールアドレスを設定すべきではないためです。EメールアドレスはSSL証明書の識別子として使用されるため、すべてのEメールアドレスはシステム内で一意でなければなりません。

> **重要 -** ユーザオブジェクトが自動作成されたユーザに対する認証(ユーザが何者であるかを判断するためのアクション)と権限付与(ユーザが何を許可されているかを判断するためのアクション)は、常にリモートのバックエンドサーバ/ディレクトリサービス上で実行されます。そのため、対応するバックエンドサーバが使用不能な場合や、そのリモートサイトでユーザオブジェクトが削除されている場合には、Astaro Security Gatewayで自動的に作成されたユーザオブジェクトは機能しません。

また、Active Directoryの*シングルサインオン*(SSO)を除き、Astaro Security Gatewayはリモート認証サーバから取得したユーザ認証データを300秒間キャッシュします。このため、リモートユーザ設定への変更は、キャッシュの期限が切れた後で初めて有効になります。

認証キャッシュ

Astaro Security Gatewayが不明ユーザから`http`などのユーザ要求を受信し、認証が必要である場合は、Astaro User Authentication(AUA)が必ず認証キャッシュにエントリを書き込みます。長期的に、ユーザが頻繁に変わるような環境では、適宜キャッシュを空にすることが合理的です。また、すべてのユーザに対して、新たな認証を今すぐ強制したい場合には、【*認証キャッシュのクリア(Flush Authentication Cache)*】ボタンを使用して、認証キャッシュを空にしてください。

認証は300秒間有効です。この間、同じユーザから他の認証要求があったときには、直接キャッシュが検索されます。この方法により、eDirectoryなどのバックエンド認証サービスにかかる負荷を軽減できます。

注 - キャッシュのフラッシングは、リモートログイン中のユーザには影響がありません。

ライブログ

ライブログを開く(Open Live Log): このボタンをクリックすると、新しいウィンドウに*Astaro User Authentication*(AUA)のログが表示されます。

5.6.2サーバ

【定義(Definitions)】&*【ユーザ(Users)】*>>*【認証サーバ(Authentication Servers)】*>>*【サーバ(Servers)】*タブで、1つ以上の認証サーバ(eDirectory、Active Directory、LDAP、RADIUS、TACACS+など)を作成できます。

5.6.2.1 eDirectory

Novell eDirectoryは、あるネットワーク内の複数のサーバとコンピュータ上にあるリソースへのアクセスを一元管理するためのX.500互換ディレクトリサービスです。eDirectoryは階層構造のオブジェクト指向データベースであり、組織内のすべての資産を論理ツリーで表現します。資産には、人、サーバ、ワークステーション、アプリケーション、プリンタ、サービス、グループなどが含まれます。

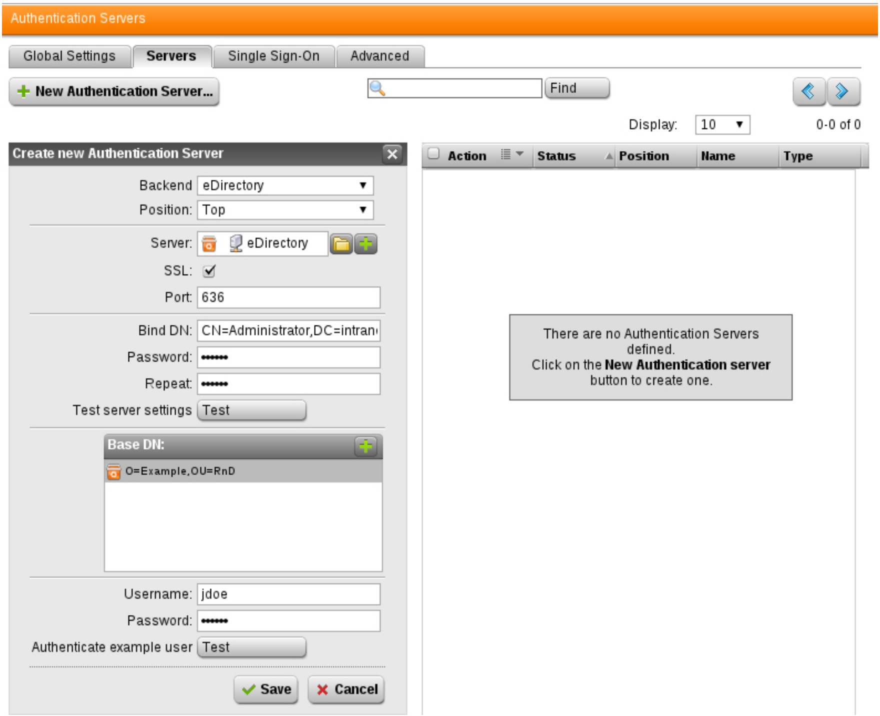


図39　認証(Authentication):eDirectoryの設定

eDirectory認証を設定するには、次の手順に従ってください。

1. ***【サーバ(Servers)】タブで、【新規認証サーバ(New Authentication Server)】をクリックします。***
   *【新規認証サーバの作成(Create New Authentication Server)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド(Backend): バックエンドのディレクトリサービスとして*【eDirectory】*を選択します。

   位置(Position): バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ(Server): eDirectoryサーバを選択(または追加)します。

SSLを使用(Use SSL)：SSLデータ転送を有効にするには、このオプションを選択します。すると、*ポート*が389(LDAP)から636(ldaps = LDAP over SSL)に変わります。

ポート(Port): eDirectoryサーバのポートを選択します。デフォルトで、ポート389が選択されています。

バインドDN(Bind DN): サーバにバインドするユーザの*識別名*(DN)を指定します。eDirectoryサーバへの匿名での問い合わせが許可されていない場合、このユーザが必要です。バインドユーザには、関連するすべてのユーザオブジェクト情報をeDirectoryサーバから取得してユーザの認証を行うために必要な特権が付与されている必要があります。eDirectoryユーザ、グループ、コンテナは、LDAP表記法で完全識別名として指定します。区切り文字にはコンマを使用します(
例：CN=administrator,DC=intranet,DC=example,DC=com)。

パスワード(Password): バインドユーザのパスワードを入力します(確認のために2回)。

サーバ設定のテスト(Test Server Settings)：【*テスト(Test)*】ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。このボタンは、【*適用(Apply)*】ボタンをクリックしてサーバ設定を保存した場合のみ使用できます。

ベースDN(Base DN): LDAPツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベースDNは、LDAP表記の完全識別名(FDN)で、コンマを区切り文字として使用して指定する必要があります(例：O=Example,OU=RnD)。ベースDNは空にすることもできます。この場合は、ベースDNは自動的にディレクトリから取り出されます。

ユーザ名(Username): 認証を実行するテストユーザのユーザ名を入力してください。

パスワード(Password): テストユーザのパスワードを入力します。

サンプルユーザの認証(Authenticate Example User)：【*テスト(Test)*】ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***【保存(Save)】*をクリックします。**
   サーバが【*サーバ(Servers)*】リストに表示されます。

5.6.2.2Active Directory

Active Directory(AD)とは、マイクロソフトが実装したディレクトリサービスであり、Windows 2000/2003 Serverの中核を成すコンポーネントです。Active Directoryには、ユーザ、グルー

プ、コンピュータ、プリンタ、アプリケーション、サービス、あらゆる種類のユーザ定義オブジェクトなど、ネットワーク内に存在するさまざまなリソースに関する情報が保存されます。このため、Active Directoryには、これらのリソースへのアクセスを一元的に体系化し、管理し、コントロールするための機能が用意されています。

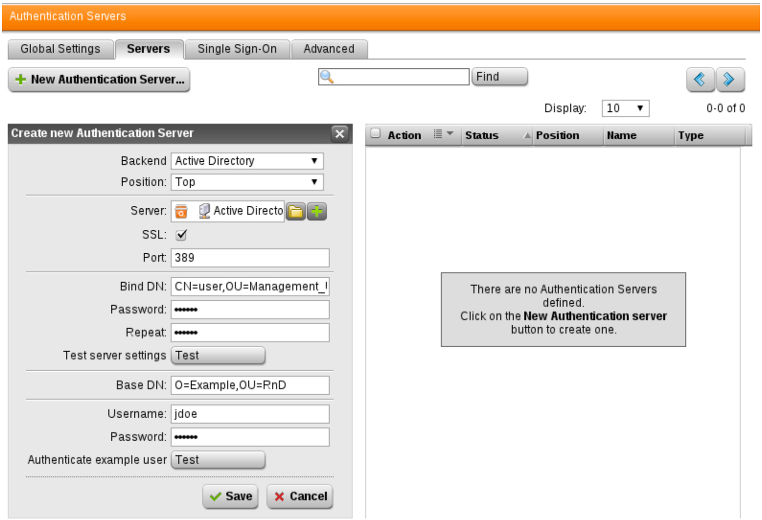


図 40 認証(Authentication):Active Directoryユーザ認証の設定

Active Directory認証方式では、Astaro Security GatewayをWindowsドメインに登録し、プライマリのドメインコントローラ(DC)にAstaro Security Gateway用のオブジェクトを作成します。これにより、ASGは、このドメインのユーザとグループに関する情報を問い合わせることが可能になります。

Active Directory認証を設定するには、次の手順に従ってください。

1. ***【サーバ(Servers)】タブで、【新規認証サーバ(New Authentication Server)】をクリックします。***
   *【新規認証サーバの作成(Create New Authentication Server)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド(Backend): バックエンドのディレクトリサービスとして*【Active Directory】*を選択します。

位置(Position): バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

サーバ(Server): Active Directoryサーバを選択(または追加)します。

SSLを使用(Use SSL):SSLデータ転送を有効にするには、このオプションを選択します。すると、*ポート*が389(LDAP)から636(ldaps = LDAP over SSL)に変わります。

ポート(Port): Active Directoryサーバのポートを選択します。デフォルトで、ポート389が選択されています。

サーバ設定のテスト(Test Server Settings):*【テスト(Test)】*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。このボタンは、*【適用(Apply)】*ボタンをクリックしてサーバ設定を保存した場合のみ使用できます。

バインドDN(Bind DN): サーバにバインドするユーザの完全な*識別名*(DN)をLDAP表記法で指定します。eDirectoryサーバへの匿名での問い合わせが許可されていない場合、このユーザが必要です。バインドユーザには、関連するすべてのユーザオブジェクト情報をActive Directoryサーバから取得してユーザの認証を行うために必要な特権を付与する必要があります。通常は、ドメインの管理者がこの要件に対応します。

各DNは、Active Directoryユーザオブジェクトのいくつかの属性から成る1つ以上のRDN(*相対識別名*)で構成されます。ユーザ名、常駐するノード、サーバのトップレベルDNなどを、コンマ区切りのLDAP表記法で記述します。

- ユーザ名は、ディレクトリにアクセスできるユーザの名前にする必要があり、CN識別子(CN=userなど)で指定します。ドメイン権限を持つ「admin」などの一般的なアカウントを使用することもできますが、ベストプラクティスとしては、admin権限を持たないユーザを指定することが推奨されます。この理由は、所与のベースDNを起点とするサブツリー内の全オブジェクトに対する読み取り権限さえあれば十分であるためです。

- ユーザオブジェクトが保存されているノードの情報には、ルートノードからユーザオブジェクトまですべてのサブノードが含まれている必要があり、通常はいわゆる*組織ユニット*コンポーネントや一*般名*コンポーネントから構成されます。組織ユニット(Microsoft Management Consoleでは、フォルダと本を組み合わせたアイコンで示される)は、識別子OUを使用して指定します。ノードは、最も低いノードから順に並べられ、末尾は最も高いノードになります。つまり、先頭は最も詳細な要素になります(例:OU=Management_US,OU=Management)。一方、事前定義されてい

るUsersノードなどのデフォルトActive Directoryコンテナ(シンプルなフォルダアイコンで示される)は、識別子`CN`で指定します(例:`CN=Users`)。

- サーバのトップレベルDNは、それぞれ識別子`DC`で指定されている複数のドメインコンポーネントから構成することができます。ドメインコンポーネントはドメイン名と同じ順序で指定します(たとえば、ドメイン名が`example.com`である場合、DN部分は`DC=example,DC=com`とします)。

たとえば、名前が`administrator`であり、オブジェクトが`example.com`ドメインの`Users`コンテナに保存されるバインドユーザのDNは次のようになります。`CN=administrator,CN=Users,DC=example,DC=com`

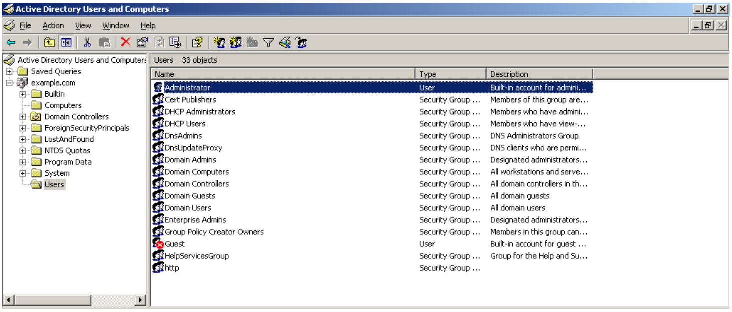


図41 認証(Authentication):Microsoft Management Console

ここで、*Management*という名前の組織ユニットを作成し、サブノードを*Management_US*とし、管理者ユーザオブジェクトをこのサブノードに移動すると、管理者のDNは次のように変わります。`CN=administrator,OU=Management_US,OU=Management,DC=example,DC=com`

パスワード(Password): バインドユーザのパスワード(確認のために2回)。

サーバ設定のテスト(Test Server Settings):[*テスト(Test)*]ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。このボタンは、[*適用(Apply)*]ボタンをクリックしてサーバ設定を保存した場合のみ使用できます。

ベースDN(Base DN): LDAPツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベースDNは、LDAP表記の完全識別名(FDN)で、コンマを区切り文字として使用して指定する必要があります(例:`O=Example,OU=RnD`)。ベースDNは空にすることもできます。この場合は、ベースDNは自動的にディレクトリから取り出されます。

ユーザ名(Username): 認証を実行するテストユーザのユーザ名を入力してください。

パスワード(Password): テストユーザのパスワードを入力します。

サンプルユーザの認証(Authenticate Example User):［*テスト(Test)*］ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***［保存(Save)］をクリックします。***
   サーバが［*サーバ(Servers)*］リストに表示されます。

5.6.2.3LDAP

LDAPとは、「*Lightweight Directory Access Protocol*」の略であり、X.500標準に基づいてディレクトリサービスの問い合わせと変更を行うネットワーキングプロトコルです。Astaro Security Gateway では、複数のサービスへのユーザ認証にLDAPプロトコルを使用しており、LDAPサーバに設定された属性やグループメンバシップに基づいてアクセスを許可または却下します。

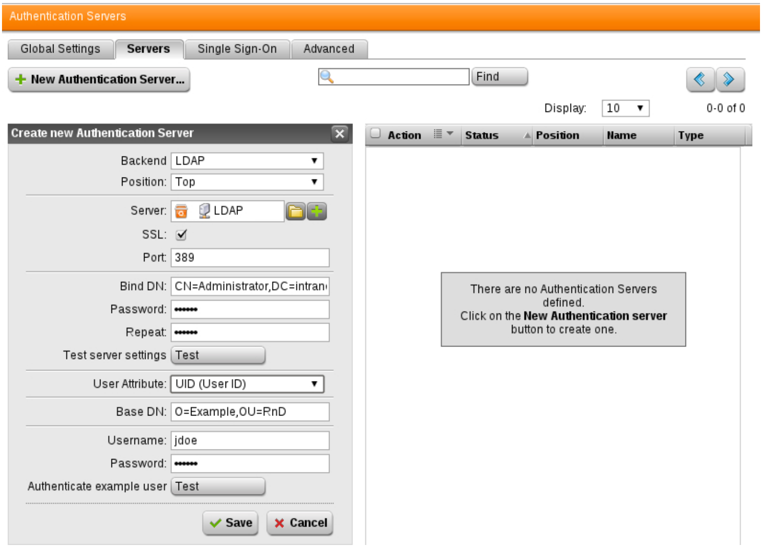


図42　認証(Authentication):LDAPの設定

LDAP認証を設定するには、次の手順に従ってください。

1. ***【サーバ(Servers)】タブで、【新規認証サーバ(New Authentication Server)】をクリックします。***
   *【新規認証サーバの作成(Create New Authentication Server)】*ダイアログボックスが開きます。
2. **次の設定を行います。**
   バックエンド(Backend): バックエンドのディレクトリサービスとして*【LDAP】*を選択します。

   位置(Position): バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ(Server): LDAPサーバを選択(または追加)します。

   SSLを使用(Use SSL): SSLデータ転送を有効にするには、このオプションを選択します。すると、*ポート*が`389`(LDAP)から`636`(ldaps = LDAP over SSL)に変わります。

   ポート(Port): LDAPサーバのポートを選択します。デフォルトでは、ポート`389`が選択されています。

   バインドDN(Bind DN): サーバにバインドするユーザの*識別名*(DN)を指定します。このユーザは必須です。セキュリティ上の理由から、LDAPサーバへの匿名での問い合わせはサポートされていません。バインドユーザには、関連するすべてのユーザオブジェクト情報をLDAPサーバから取得してユーザを認証するために必要な特権が付与されている必要があります。LDAPユーザ、グループ、コンテナは、LDAP表記法で完全識別名として指定します。区切り文字にはコンマを使用します。(
   例:`CN=administrator,DC=intranet,DC=example,DC=com`)

   パスワード(Password): バインドユーザのパスワードを入力します(確認のために2回)。

   サーバ設定のテスト(Test Server Settings):*【テスト(Test)】*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。このボタンは、*【適用(Apply)】*ボタンをクリックしてサーバ設定を保存した場合のみ使用できます。

   ユーザ属性(User Attribute): LDAPディレクトリ検索用のフィルタとして使用されるユーザ属性を選択します。ユーザ属性には、リモートアクセスサービスなどが各ユーザに対してプロンプト表示する実際のログイン名が含まれます。次のユーザ属性を選択できます。

   - CN(一般名)
   - SN(姓)

- UID(ユーザID)

LDAPディレクトリのユーザ名がこれらのフォームに保存されていない場合、リストで*<<カスタム(Custom)>>*を選択し、下の【*カスタム(Custom)*】フィールドにカスタム属性を入力します。この属性はLDAPディレクトリで設定する必要があります。

ベースDN(Base DN): LDAPツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベースDNは、LDAP表記の完全識別名(FDN)で、コンマを区切り文字として使用して指定する必要があります(例:`O=Example,OU=RnD`)。ベースDNは空にすることもできます。この場合は、ベースDNは自動的にディレクトリから取り出されます。

ユーザ名(Username): 認証を実行するテストユーザのユーザ名を入力してください。

パスワード(Password): テストユーザのパスワードを入力します。

サンプルユーザの認証(Authenticate Example User):【*テスト(Test)*】ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***【保存(Save)】をクリックします。***
   サーバが【*サーバ(Servers)*】リストに表示されます。

5.6.2.4RADIUS

RADIUSとは、「*Remote Authentication Dial In User Service*」の略であり、ルータなどのネットワークデバイスで中央データベースに対してユーザを認証するために広く用いられているプロトコルです。RADIUSには、ユーザの情報に加え、ネットワークデバイスで使用される技術情報(サポートされるプロトコル、IPアドレス、ルーティング情報など)も保存できます。この情報は、RADIUSサーバ上のファイルまたはデータベースに保存されるユーザプロファイルを構成します。

RADIUSプロトコルは非常に柔軟であり、サーバはほとんどのオペレーティングシステムで利用可能です。このASGにRADIUSを導入することで、プロキシとユーザに基づいてアクセス権限を設定できるようになります。RADIUS認証を使用するためには、ネットワーク上で稼働しているRADIUSサーバが必要です。パスワードは平文(暗号化なし)で送信されるため、ASGと同じネットワーク内にRADIUSサーバを配置してください。また、ASGとサーバは同じスイッチに接続してください。

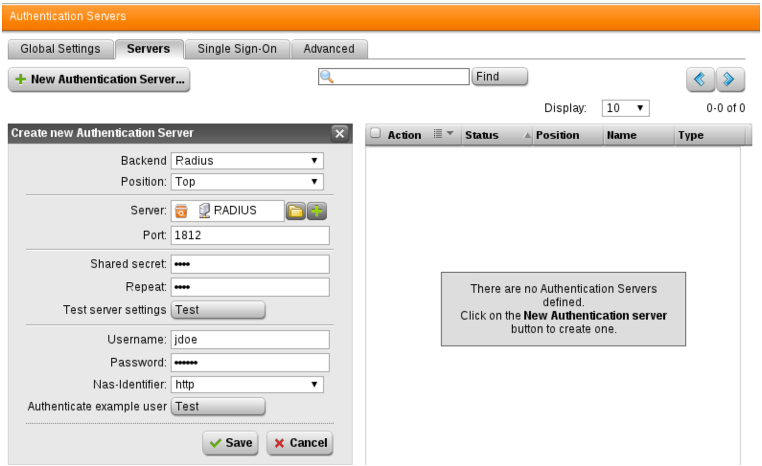


図43　認証(Authentication):RADIUSの設定

RADIUS認証を設定するには、次の手順に従ってください。

1. ***【サーバ(Servers)】タブで、【新規認証サーバ(New Authentication Server)】をクリックします。***
   *【新規認証サーバの作成(Create New Authentication Server)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド(Backend): バックエンドのディレクトリサービスとして*【RADIUS】*を選択します。

   位置(Position): バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ(Server): RADIUSサーバを選択(または追加)します。

   ポート(Port): RADIUSサーバのポートを選択します。デフォルトでは、ポート1812が選択されています。

   共有シークレット(Shared Secret): 共有シークレットとは、RADIUSクライアントとRADIUSサーバの間でパスワードとしての役割を果たすテキスト文字列です。共有シークレットを入力します(確認のために2回)。

サーバ設定のテスト(Test Server Settings):【*テスト(Test)*】ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。

ユーザ名(Username): 認証を実行するテストユーザのユーザ名を入力してください。

パスワード(Password): テストユーザのパスワードを入力します。

NAS識別子(NAS Identifier): 適切なNAS識別子をリストから選択します。詳細は、注記と下の表を参照してください。

サンプルユーザの認証(Authenticate Example User):【*テスト(Test)*】ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***【保存(Save)】をクリックします。***
サーバが【*サーバ(Servers)*】リストに表示されます。

注 -RADIUSサーバに問い合わせを行う、Astaro Security Gatewayの各ユーザ認証サービス(PPTPやL2TP)は、異なる識別子(NAS識別子)をRADIUSサーバに送信します。たとえば、PPTPサービスは、このユーザの認証を試みるときに、`pptp`というNAS識別子をRADIUSサーバに送信します。これにより、RADIUSサーバがさまざまなサービスを識別して特定の種類のサービスをユーザに付与することができるため、権限付与の目的で役に立ちます。ユーザ認証サービスとそれに対応するNAS識別子のリストは以下のとおりです。

ユーザ認証サービス	NAS識別子
SSL VPN	`ssl`
PPTP	`pptp`
IPsec	`ipsec`
L2TP over IPsec	`l2tp`
SMTPプロキシ	`smtp`
ユーザポータル	`portal`
WebAdmin	`webadmin`

ユーザ認証サービス	NAS識別子
SOCKSプロキシ	socks
Webフィルタ	http
認証クライアント	エージェント

表1:RADIUS NAS識別子

5.6.2.5TACACS+

TACACS+(「*Terminal Access Controller Access Control System*」の略)語)とは、Cisco Systems, Inc.独自のプロトコルであり、認証プロセスと権限付与プロセスについて詳細なアカウンティング情報と管理的なコントロールを提供します。RADIUSでは認証と権限付与がユーザプロファイルにまとめられていますが、TACACS+ではこれらのオペレーションを区別しています。他の相違点としては、TACACS+ではTCPプロトコル(ポート49)を使用し、RADIUSではUDPプロトコルを使用します。

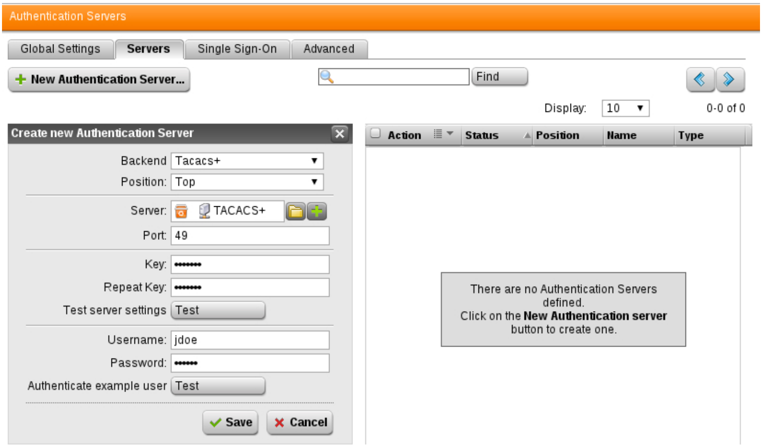


図44 認証(Authentication):TACACS+ユーザ認証の設定

TACACS+認証を設定するには、次の手順に従ってください。

1. ***【サーバ(Servers)】タブで、【新規認証サーバ(New Authentication Server)】をクリックします。***

*【新規認証サーバの作成(Create New Authentication Server)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド(Backend): バックエンドのディレクトリサービスとして*【TACACS+】*を選択します。

   位置(Position): バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ(Server): TACACS+サーバを選択(または追加)します。

   ポート(Port): TACACS+サーバのポートを選択します。デフォルトでは、ポート`49`が選択されています。

   鍵(Key):Astaro Security GatewayとTACACS+サーバの間のすべてのTACACS+通信に使用する認証および暗号鍵を入力します。ここで入力する鍵の値は、TACACS+サーバで設定した値と一致している必要があります。鍵を入力してください(確認のために2回)。

   サーバ設定のテスト(Test Server Settings):*【テスト(Test)】*ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。このボタンは、*【適用(Apply)】*ボタンをクリックしてサーバ設定を保存した場合のみ使用できます。

   ユーザ名(Username): 認証を実行するテストユーザのユーザ名を入力してください。

   パスワード(Password): テストユーザのパスワードを入力します。

   サンプルユーザの認証(Authenticate Example User):*【テスト(Test)】*ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. ***【保存(Save)】*をクリックします。**
   サーバが*【サーバ(Servers)】*リストに表示されます。

5.6.3シングルサインオン(Single Sign-On)

*【定義(Definitions)】&【ユーザ(Users)】>>【認証サーバ(Authentication Servers)】>>【シングルサインオン(Single Sign-On)】*タブでは、Active DirectoryまたはeDirectory(あるいはその両方)のシングルサインオン機能を設定できます。

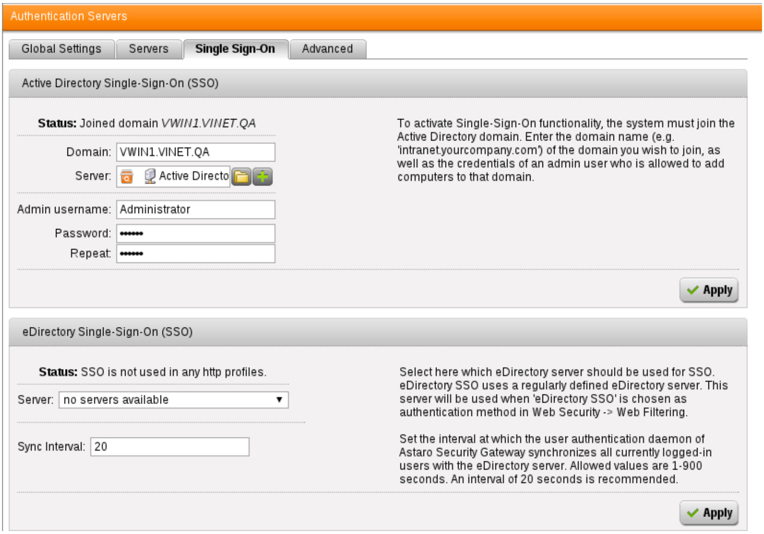


図45 認証(Authentication):シングルサインオンの設定

Active DirectoryのシングルサインオンSSO(SSO)

Active DirectoryのSSO機能は現在、Webフィルタのみで使用されており、NTLMv2またはKerberos認証をサポートするブラウザでシングルサインオン機能を使用できます。

シングルサインオン機能を有効にするには、ASGをActive Directoryドメインに追加する必要があります。追加するドメインが機能するためには、次の前提条件を満たしている必要があります。

- ゲートウェイとドメインコントローラ(DC)のタイムゾーンが同じである。
- ゲートウェイのクロックとDCのクロックの間に、5分を超える時刻差がない。
- ASGホスト名がADDNSシステムに存在する。
- ASGがAD DNSをフォワーダとして使用しているか、ADドメインのDNS要求ルートがAD DNSサーバをポイントしている。

Active Directory SSOを設定するには、次の手順に従ってください。

1. **Active Directoryサーバを*【サーバ(Servers)】*タブで作成します。**
2. **次の設定を行います。**
   ドメイン(Domain): ドメインの名前(`intranet.mycompany.com`など)。

サーバ(Server)(オプション):ASGで特定のDCを使用するには、ここでActive Directoryサーバを選択(または追加)してください。ここで指定しなければ、ASGはDNS経由で取得可能なすべてのDCを使用します。

adminユーザ名(Admin Username): 管理特権があり、ドメインにコンピュータを追加することが許可されているユーザ(通常は「管理者」)。

パスワード(Password): adminユーザのパスワード(確認のために2回)。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

Kerberos認証サポートに関する注記:SSO Kerberosサポートが機能するためには、クライアントはプロキシ設定でASGのFQDNホスト名を使用する必要があります。IPアドレスを使用すると機能しません。NTLMv2モードは、この要件の影響を受けません。この要件が満たされていない場合や、ブラウザがKerberos認証をサポートしない場合には、NTLMv2モードが自動的に使用されます。

eDirectoryのシングルサインオン(SSO)

ここでは、eDirectory用にSSOを設定できます。*【Webセキュリティ(Web Security)】*>>*【Webフィルタリング(Web Filtering)】*で認証方式として*eDirectory SSO*を設定した場合、ここで選択したeDirectoryサーバが使用されます。

eDirectory SSOを設定するには、次の手順に従ってください。

1. **eDirectoryサーバを*【サーバ(Servers)】*タブに登録します。**
2. **eDirectoryサーバを選択します。**
   SSOを有効にしたいeDirectoryサーバをドロップダウンリストで選択します。
3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

5.6.4詳細

パスワードの複雑性(Password Complexity)

このオプションを使用すると、管理者や管理者権限を持つローカル登録ユーザに対して、パスワードの強化を強制できます。次のセキュリティ要件を遵守するパスワードの複雑性を設定できます。

- パスワードの最低長。デフォルトは8文字
- 小文字が1つ以上必要
- 大文字が1つ以上必要
- 数字が1つ以上必要
- 英数字以外の文字が1つ以上必要

選択したパスワードプロパティを有効にするためには、【*複雑なパスワードを必須にする(Require complex passwords)*】チェックボックスにチェックを入れて、【*適用(Apply)*】をクリックします。

ディレクトリユーザのプリフェッチ(Prefetch Directory Users)

eDirectoryまたはActive DirectoryのユーザをASGと同期することができます。これにより、ASGにユーザオブジェクトが事前に作成され、当該ユーザがログインしたときには、これらのユーザオブジェクトがすでに存在しています。同期プロセスは週次または日次で実行できます。

プリフェッチを有効にするには、次の設定を行います。

サーバ(Server): このドロップダウンリストには、【*サーバ(Servers)*】タブで作成されたサーバが含まれています。プリフェッチを有効にするサーバを選択します。

プリフェッチ間隔(Prefetch Interval): ユーザをプリフェッチする間隔を選択します。同期を週次で実行する場合、同期を開始する曜日を選択します。同期を日次で実行する場合、【*デイリー(Daily)*】を選択します。

プリフェッチ時間(Prefetch Time): ユーザをプリフェッチする時間を選択します。

eDirectory/Active Directoryグループ(eDirectory/Active Directory Groups): どのグループを事前に作成するか指定するには、ここでグループを入力します。統合LDAPブラウザを使用して、これらのグループを選択できます。

ログイン時のバックエンド同期を有効にする(Enable Backend Sync on Login)(オプション): 不明ユーザのログイン時に、ディレクトリからユーザ情報をフェッチする場合には、このオプションを選択します。

設定を保存するには【*適用(Apply)*】をクリックします。

直ちにプリフェッチ(Prefetch Now): プリフェッチを今すぐ開始するには、このボタンをクリックします。

開く(Open): プリフェッチのライブログを開くには、このボタンをクリックします。

6インタフェースおよびルーティング

この章では、Astaro Security Gatewayでインタフェースとネットワーク固有の設定を構成する方法について説明します。WebAdminの【*ネットワーク統計(Network Statistics)*】ページには、今日の上位10件のアカウンティングサービス、上位送信元ホスト、および同時接続の概要が表示されます。各セクションには、【*詳細(Detail)*】リンクが含まれています。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

この章には次のトピックが含まれます。

- インタフェース
- ブリッジング
- スタティックルーティング
- ダイナミックルーティング(OSPF)
- IPv6
- サービス品質(QoS)
- マルチキャストルーティング(PIM-SM)
- アップリンクモニタリング

6.1 インタフェース

ファイアウォールには、内部LANを外部ネットワーク(インターネットなど)にセキュリティを維持して接続するために、少なくとも2つのネットワークインタフェースカードが必要です。次の例では、ネットワークカード`eth0`は、常に内部ネットワークに接続されるインタフェースであり、ネットワークカード`eth1`は、外部ネットワーク(インターネットなど)に接続されるインタフェースです。これらのインタフェースは、それぞれ信頼されるインタフェース、信頼されないインタフェースとも呼ばれます。

ネットワークカードは、インストール中に自動認識されます。ソフトウェアアプライアンスでは、新しいネットワークカードを後で追加する場合、新たなインストールが必要になります。システムの再インストールを行うには、設定のバックアップをとり、ソフトウェアをインストールし、バックアップを復元するだけです。

ゲートウェイを内部ネットワークと外部ネットワークの唯一の接点としなければなりません。すべてのデータはASGを通過する必要があります。内部インタフェースと外部インタフェースを1つのハブまたはスイッチに接続することはお勧めしません。ただし、スイッチがVLANスイッチとして設定されている場合は除きます。誤ったARP(アドレス解決プロトコル)解決が発生する可能性があり、これを「ARPクラッシュ」と呼びます。この状況は、(マイクロソフト製品など)オペレーティングシステムによっては管理できないものもあります。そのため、各ゲートウェイネットワークインタフェースに対して、1つの物理ネットワークセグメントを使用する必要があります。

【*インタフェース(Interfaces)*】メニューを使用すると、ASGにインストールされているすべてのネットワークカードを設定・管理したり、外部ネットワーク(インターネット)へのすべてのインタフェースや内部ネットワーク(LAN、DMZ)へのインタフェースを設定・管理することができます。

注 - ネットワークトポロジを計画し、ASGを設定しているときは、どのインタフェースをどのネットワークに接続しているかに注意してください。ほとんどの設定で、SysIDが`eth1`のネットワークインタフェースは外部ネットワークへの接続として選択されます。高可用性(HA)フェイルオーバーをインストールするためには、同じSysIDのネットワークカードを両システムで選択する必要があります。HAフェイルオーバーのインストールについては、「*冗長化*」のページで詳しく説明しています。

次のセクションでは、【*インタフェース(Interfaces)*】、【*追加アドレス(Additional Addresses)*】、【*リンクアグリゲーション(Link Aggregation)*】、【*アップリンクバランシング(Uplink Balancing)*】、【*マルチパスルール(Multipath Rules)*】、【*ハードウェア(Hardware)*】のタブを使用してさまざまなインタフェースタイプを管理および設定する方法について説明します。

6.1.1 インタフェース

【*インタフェース(Interfaces)*】タブでは、ネットワークカードと仮想インタフェースを設定できます。リストに、すでに定義されているインタフェースが、シンボル名、ハードウェアデバイス、現在のアドレスとともに表示されます。インタフェースのステータスも表示されます。ステータスアイコンをクリックして、インタフェースを有効または無効にすることができます。

ヒント -【*インタフェース(Interfaces)*】リストでインタフェース定義の情報アイコンをクリックすると、インタフェース定義が使用されているすべての設定オプションを表示することができます。

新たに追加されたインタフェースは、セットアップ中、【*ダウン(Down)*】と表示される可能性があります。対応するボタンをクリックして、インタフェースを編集したり削除することができます。

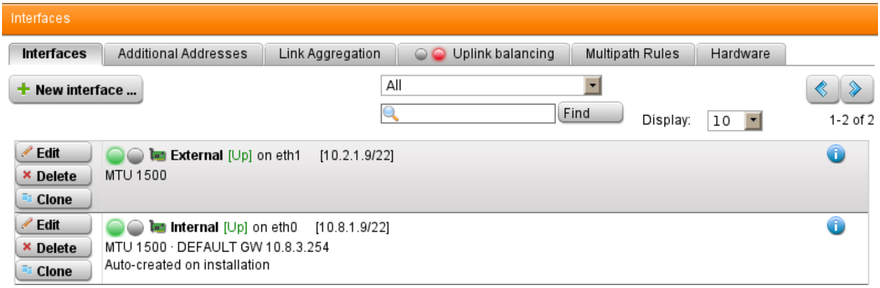


図46 インタフェース(Interfaces):インタフェースの設定

6.1.1.1 自動インタフェースネットワーク定義

ゲートウェイの各インタフェースには、シンボル名とハードウェアデバイスが割り当てられています。シンボル名は、他の構成設定でインタフェースを参照するときに使用します。各インタフェースについて、次のような対応するネットワーク定義のセットがゲートウェイによって自動的に作成されます。

- インタフェースの現在のIPアドレス、インタフェース名と*(アドレス(Address))*サフィックスから成る名前が含まれる定義。
- インタフェースに接続されたネットワーク、インタフェース名と*(ネットワーク(Network))*サフィックスから成る名前が含まれる定義。この定義は、PPP*(ポイントツーポイント)*タイプのインタフェースに対しては作成されません。
- インタフェースのブロードキャストアドレス、インタフェース名と*(ブロードキャスト(Broadcast))*サフィックスから成る名前が含まれる定義。この定義は、PPP*(ポイントツーポイント)*タイプのインタフェースに対しては作成されません。

インタフェースで動的アドレス割り当て方法(DHCPやリモート割り当てなど)が使用されている場合、これらの定義は自動的に更新されます。ファイアウォールやNATルールなど、これらの定義を参照するすべての設定も、変更されたアドレスで自動的に更新されます。

*「内部(Internal)」*というシンボル名のインタフェースが1つあらかじめ定義されています。これはマネジメントインターフェースであり、通常は「内部」ゲートウェイインタフェースとして使用されます。名前を変更したい場合は、インストール直後に行う必要があります。

6.1.1.2インタフェースタイプ

以下のリストに、ゲートウェイに追加できるインタフェースタイプと、それらをサポートするために必要なハードウェアのタイプを示します。

3G/UMTS:これは、USBモデムスティックに基づくインタフェースです。スティックは差し込む必要があり、ASGはインタフェース作成前にリブートする必要があります。

標準イーサネット(Ethernet Standard):これは標準のイーサネットインターフェースで、10、100、あるは1000Mbpsの帯域幅を備えています。

イーサネットVLAN(Ethernet VLAN):VLAN(仮想LAN)は単一のハードウェアインタフェース上に別個のレイヤ2ネットワークセグメントを複数持つ方式です。各セグメントは整数の「タグ」で識別されます。VLANインタフェースを追加するときは、さらなるインタフェース(エイリアス)の追加に使用できる「ハードウェア」デバイスを作成します。PPPoEおよびPPPoAデバイスはVLAN仮想ハードウェア上では実行できません。

ケーブルモデム(DHCP)(Cable Modem(DHCP)):これはDHCPを使用した標準イーサネットインタフェースです。

DSL(PPPoE):PPP over Ethernet。DSL PPPoEデバイスでは、ゲートウェイを*PPP-over-Ethernet*互換のDSL回線に接続できます。これらのデバイスには専用イーサネット接続が必要です(同じハードウェア上で他のインタフェースと共存できません)。DSLモデムをインタフェースネットワークセグメントに接続する必要があります。これらのデバイスタイプのネットワークパラメータは、リモートステーションで割り当てることができます(一般的にはご利用のISP)。さらに、ISPアカウントのユーザ名およびパスワードを入力する必要があります。

DSL(PPPoA/PPTP):PPP over ATM。DSL PPPoAデバイスでは、ゲートウェイを*PPP-over-ATM*互換のDSL回線に接続できます。これらのデバイスはPPTプロトコルを使用してIPパケットをトンネリングします。これらのデバイスには専用イーサネット接続が必要です(同じハードウェア上で他のインタフェースと共存できません)。DSLモデムをインタフェースネットワークセグメントに接続する必要があります。これらのデバイスタイプのネットワークパラメータは、リモートステーションで割り当てることができます(一般的にはご利用のISP)。さらに、ISPアカウントのユーザ名およびパスワードを入力する必要があります。また、お使いのモデムのIPアドレスも入力する必要があります。このアドレスは通常モデムに組み込まれているため変更できません。モデムで通信するには、NIC IPアドレスとネットマスクを入力する必要があります。モデムのIPアドレスは、これらのパラメータで定義されたネットワーク内であることが必要です。*Pingアドレス*はICMP ping要求に応答するPPTPリンクの反対側のホストであることが必要です。ご利用のISPのDNSサーバを使用することができます。このアドレスでpingできなかった場合、接続がデッド(dead)であることが考えられ、これは再開されます。

モデム(PPP):このタイプのインタフェースでは、PPPモデムを介してASGをインターネットに接続できます。設定するためには、ASGにシリアルインタフェースと外部モデムが必要です。また、ユーザ名とパスワードを含むDSLアクセスデータも必要です。これらのデータはISPから入手できます。

6.1.1.33G/UMTS

内部または外部ネットワークにイーサネット接続するためのネットワークカードを設定するには、NIC及びIPアドレスとネットマスクを設定する必要があります。

標準イーサネットインタフェースを設定するには、次の手順に従ってください。

1. **【インタフェース(Interfaces)】タブで、【新規インタフェース(New Interface)】をクリックします。**【*新規インタフェースの作成(Create New Interface)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): インタフェースを説明する名前を入力します。

   タイプ(Type): ドロップダウンリストから【*Ethernet Standard(Ethernet Standard)*】を選択します。

   ハードウェア(Hardware): ドロップダウンリストからUSBモデムを選択します。USBスティックを差し込んだ後で、リブートする必要があります。

   ネットワーク(Network): モバイルネットワークタイプを*GSM/W-CDMA*または*CDMA*から選択します。

   IPv4デフォルトGW(IPv4 Default GW)(オプション):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   PIN(オプション):PINが設定されている場合、SIMカードのPINを入力します。

   APN自動選択(APN Autoselect):(オプション):デフォルトで、使用するAPN(アクセスポイント名)はUSBモデムスティックから取得されます。チェックボックスのチェックを外す場合、【*APN*】フィールドにAPN情報を入力します。

   ユーザ名/パスワード(Username/Password)(オプション):必要な場合、モバイルネットワークのユーザ名とパスワードを入力します。

   ダイヤル文字列(Dial String)(オプション):プロバイダが異なるダイヤル文字列を使用している場合、ここに入力します。デフォルトは`*99#`です。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
   初期化文字列(Init String): USBモデムスティックを初期化するための文字列を入力します。USBモデムスティックに応じて初期化文字列の調整が必要になる可能性があります。この場合、初期化文字列は当該USBモデムスティックのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

   リセット文字列(Reset String): USBモデムスティックのリセット文字列を入力します。USBモデムスティックに応じてリセット文字列の調整が必要になる可能性があります。この

場合、リセット文字列は当該USBモデムスティックのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトで、*3G/UMTS*インタフェースタイプには1500バイトのMTUが設定されています。

非対称(Asymmetric)(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(Displayed Max)(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***【保存(Save)】*をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

5. **インタフェースを有効にします。**

   インタフェースを有効にするには、ステータスアイコンをクリックします。

   これでインタフェースが有効になります(ステータスアイコンは緑色)。まだインタフェースが*【ダウン(Down)】*と表示されている場合もあります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*【アップ(Up)】*メッセージが表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.4イーサネット標準

内部または外部ネットワークにイーサネット接続するためのネットワークカードを設定するには、NIC及びIPアドレスとネットマスクを設定する必要があります。

標準イーサネットインタフェースを設定するには、次の手順に従ってください。

1. **【*インタフェース(Interfaces)*】タブで、【*新規インタフェース(New Interface)*】をクリックします。**【*新規インタフェースの作成(Create New Interface)*】ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name): インタフェースを説明する名前を入力します。

   タイプ(Type): ドロップダウンリストから【*Ethernet Standard(Ethernet Standard)*】を選択します。

   ハードウェア(Hardware): ドロップダウンリストからインタフェースを選択します。

   > **ヒント -** インターネットなどの外部接続には、SysIDがeth1のネットワードカードを選択してください。1枚のネットワークカードを、*標準イーサネットインタフェースおよびPPPoE DSL(PPP over Ethernet)*接続または*PPPoA DSL(PPTP over Ethernet)*接続として同時に使用することはできません。

   IPv4アドレス(IPv4 Address): インタフェースのIPアドレスを入力します。

   ネットマスク(Netmask): ネットマスク(IPv4)を選択するか、IPv6ネットマスクを入力します。

   IPv4/IPv6デフォルトGW(IPv4/IPv6 Default GW)(オプション):静的に定義されたデフォルトゲートウェイを使用する場合、このオプションを選択します。

   デフォルトGW IP(Default GW IP)(オプション):デフォルトゲートウェイのIPアドレスを入力します。

   > **注 -** インタフェースを設定して、IPv4およびIPv6アドレスを同時に使用することができます。

   コメント(Comment)(オプション):説明などの情報を追加します。
3. **オプションで、次の詳細設定を行います。**
   MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェー

ス)。デフォルトで、*イーサネット標準*インタフェースタイプには1500バイトのMTUが設定されています。

プロキシARP(Proxy ARP): 機能を有効にするには、チェックボックスにチェックを入れます。デフォルトでは、【*プロキシARP(Proxy ARP)*】機能は無効(オフ)になっています。
このオプションはブロードキャストタイプのインタフェースで使用できます。これを選択すると、ゲートウェイがそのインタフェース上のトラフィックをその「背後にある」ホストに対して「引きつけ」、受け渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISPのルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

非対称(Asymmetric)(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(Displayed Max)(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. **【*保存(Save)*】をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

5. **インタフェースを有効にします。**

インタフェースを有効にするには、ステータスアイコンをクリックします。

これでインタフェースが有効になります(ステータスアイコンは緑色)。まだインタフェースが【*ダウン(Down)*】と表示されている場合もあります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。【*アップ(Up)*】メッセージが表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.5イーサネットVLAN

ASGを仮想LANに接続するためには、タグ付け可能なドライバが用意されたネットワークカードが必要になります。タグとは、イーサネットヘッダの一部としてパケットに付けられる4バイトのヘッダです。タグには、パケットの送信先となるVLANの番号が格納されます。VLANの番号は12ビット数で、最大4095の仮想LANまで許可します。WebAdminでは、この数を「*VLANタグ*」と呼びます。

注 - Astaroは、タグ付け可能なネットワークインタフェースカードのリストを管理しています。*ハードウェア互換性リスト*(HCL)はAstaroナレッジベースからご利用いただけます。「HCL」を検索用語として使用して、該当するページを探してください。

イーサネットVLANインタフェースを設定するには、次の手順に従ってください。

1. ***【インタフェース(Interfaces)】タブで、【新規インタフェース(New Interface)】をクリックします。***
   *【新規インタフェースの作成(Create New Interface)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): インタフェースを説明する名前を入力します。

   タイプ(Type): ドロップダウンリストから*【Ethernet VLAN(Ethernet VLAN)】*を選択します。

   ハードウェア(Hardware): ドロップダウンリストからインタフェースを選択します。

   VLANタグ(VLAN Tag): このインタフェースに対して使用するVLANタグを入力します。

   IPv4アドレス(IPv4 Address): インタフェースのIPアドレスを入力します。

   ネットマスク(Netmask): ネットマスク(IPv4)を選択するか、IPv6ネットマスクを入力します。

   IPv4/IPv6デフォルトGW(IPv4/IPv6 Default GW)(オプション):静的に定義されたデフォルトゲートウェイを使用する場合、このオプションを選択します。

   デフォルトGW IP(Default GW IP)(オプション):デフォルトゲートウェイのIPアドレスを入力します。

   注 - インタフェースを設定して、IPv4およびIPv6アドレスを同時に使用することができます。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトで、*イーサネットVLAN*インタフェースタイプには1500バイトのMTUが設定されています。

プロキシARP(Proxy ARP): 機能を有効にするには、チェックボックスにチェックを入れます。デフォルトでは、【*プロキシARP(Proxy ARP)*】機能は無効(オフ)になっています。
このオプションはブロードキャストタイプのインタフェースで使用できます。これを選択すると、ゲートウェイがそのインタフェース上のトラフィックをその「背後にある」ホストに対して「引きつけ」、受け渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISPのルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

非対称(Asymmetric)(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(Displayed Max)(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. **【*保存(Save)*】をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

5. **インタフェースを有効にします。**

インタフェースを有効にするには、ステータスアイコンをクリックします。

これでインタフェースが有効になります(ステータスアイコンは緑色)。まだインタフェースが【*ダウン(Down)*】と表示されている場合もあります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。【*アップ(Up)*】メッセージが表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.6ケーブルモデム(DHCP)

*ケーブルモデム(DHCP)*インタフェースを設定するには、次の手順に従ってください。

1. ***【インタフェース(Interfaces)】タブで、【新規インタフェース(New Interface)】をクリックします。***
   【*新規インタフェースの作成(Create New Interface)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): インタフェースを説明する名前を入力します。

   タイプ(Type): ドロップダウンリストから【*ケーブルモデム(DHCP)(Cable Modem(DHCP))*】を選択します。

   ハードウェア(Hardware): ドロップダウンリストからインタフェースを選択します。

   ヒント - インターネットなどの外部接続には、SysIDが`eth1`のネットワードカードを選択してください。1枚のネットワークカードを、*ケーブルモデム(DHCP)*および*PPP over Ethernet*(PPPoE-DSL)または*PPTP over Ethernet*(PPPoA-DSL)接続として同時に使用することはできません。

   IPv4デフォルトGW(IPv4 Default GW)(オプション):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
   ホスト名(Hostname): ISPがシステムのホスト名の受信を要求する場合、ここに入力します。

   MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更

は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトで、*ケーブルモデム*インタフェースタイプには1500バイトのMTUが設定されています。

プロキシARP(Proxy ARP):*プロキシARP*機能を有効にするには、このオプションを選択します。これはデフォルトでは無効になっています。
このオプションはブロードキャストタイプのインタフェースで使用できます。(現在は*イーサネット標準*のみ)。これを有効にすると、ゲートウェイがそのインタフェース上のトラフィックをその「背後にある」ホストに対して「引きつけ」、受け渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISPのルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

非対称(Asymmetric)(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(Displayed Max)(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. **【*保存(Save)*】をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

5. **インタフェースを有効にします。**

   インタフェースを有効にするには、ステータスアイコンをクリックします。

   これでインタフェースが有効になります(ステータスアイコンは緑色)。まだインタフェースが【*ダウン(Down)*】と表示されている場合もあります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。【*アップ(Up)*】メッセージが表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.7DSL(PPPoE)

設定には、ご利用のISPが提供したユーザ名とパスワードを含むDSL接続情報が必要になります。VDSL もこのインタフェースタイプでサポートされています。

> **注 -** DSL接続を有効にすると、ASGはご利用のISPに1日24時間接続されます。したがって、ご利用のISPの請求が接続時間ベースではなく定額制または帯域幅ベースの料金システムであることをご確認ください。

DSL(PPPoE)インタフェースを設定するには、次の手順に従ってください。

1. ***【インタフェース(Interfaces)】タブで、【新規インタフェース(New Interface)】をクリックします。***
   *【新規インタフェースの作成(Create New Interface)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): インタフェースを説明する名前を入力します。

   タイプ(Type): ドロップダウンリストから*【DSL(PPPoE)】*を選択します。

   ハードウェア(Hardware): ドロップダウンリストからインタフェースを選択します。

   VDSL: このチェックボックスは、ご利用の接続がVDSL接続である場合のみ選択します。*MTU*は`1476`に変更されます。

   スタティックPPPoE IP(Static PPPoE IP)(オプション):ISPに割り当てられたスタティックIPアドレスがある場合、チェックボックスにチェックを入れ、表示されるテキストボックスにIPアドレスと該当するネットマスクを入力します。

   - **IPv4アドレス(IPv4 Address)**: インタフェースのIPアドレスを入力します。
   - **ネットマスク(Netmask)**: ドロップダウンリストからネットマスクを選択するか、IPv6ネットマスクを入力します(あるいはその両方)。

   > **注 -** インタフェースを設定して、IPv4およびIPv6アドレスを同時に使用することができます。

   IPv4/IPv6デフォルトGW(IPv4/IPv6 Default GW)(オプション):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   ユーザ名(Username): ISPが提供したユーザ名を入力します。

   パスワード(Password): ISPが提供したパスワードを入力します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
   毎日の再接続(Daily Reconnect): 接続を終了および再開する時間を定義します。【*無し(Never)*】を選択するか、具体的な時間を指定することができます。

   再接続遅延(Reconnect Delay): ここで、再接続遅延を変更できます。デフォルトでは、遅延は【*5秒(5 Seconds)*】に設定されています。ご利用のISPがこれより長い遅延を要求している場合は、【*1分(One Minute)*】や【*15分(Fifteen Minutes)*】に設定できます。

   MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトでは、1492バイトのMTUが【*DSL(PPPoE)*】インタフェースタイプに設定されています。

   非対称(Asymmetric)(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

   表示する最大(Displayed Max)(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. **【*保存(Save)*】をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

5. **インタフェースを有効にします。**

   インタフェースを有効にするには、ステータスアイコンをクリックします。

   これでインタフェースが有効になります(ステータスアイコンは緑色)。まだインタフェースが【*ダウン(Down)*】と表示されている場合もあります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。【*アップ(Up)*】メッセージが表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.8DSL(PPPoA/PPTP)

PPPoA(*PPP over ATM Protocolプロトコル*)した接続を設定するには、ASG上の未使用のイーサネットインタフェースと、イーサネットポート付きの外部ADSLモデムが必要です。インターネットへの接続は2つの個別の接続で行ないます。ASGとADSLモデム間では、*PPTP over Ethernetプロトコル*を使用して接続を確立します。ADSLモデムは、*PPP over ATM Dialingプロトコル*を使用してISPに接続します。

この設定には、ご利用のISPが提供したユーザ名とパスワードを含むDSL接続情報が必要になります。

注 - DSL接続を有効にすると、ASGはご利用のISPに1日24時間接続されます。したがって、ご利用のISPの請求が接続時間ベースではなく定額制または帯域幅ベースの料金システムであることをご確認ください。

DSL(PPPoA/PPTP)インタフェースを設定するには、次の手順に従ってください。

1. ***【インタフェース(Interfaces)】タブで、【新規インタフェース(New Interface)】をクリック*します。**【*新規インタフェースの作成(Create New Interface)*】ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name): インタフェースを説明する名前を入力します。

   タイプ(Type): ドロップダウンリストから【*DSL(PPPoA/PPTP)*】を選択します。

   ハードウェア(Hardware): ドロップダウンリストからインタフェースを選択します。

   IPv4デフォルトGW(IPv4 Default GW)(オプション): プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   ユーザ名(Username): ISPが提供したユーザ名を入力します。

   パスワード(Password): ISPが提供したパスワードを入力します。

   コメント(Comment)(オプション): 説明などの情報を追加します。
3. **オプションで、次の詳細設定を行います。**

モデムIP(Modem IP): お使いのADSLモデムのIPアドレスをここに入力します。このアドレスは通常、ISPから、あるいはモデムハードウェアとともに提供されるので、変更できません。例:`10.0.0.138`(AonSpeed)。

NICアドレス(NIC Address): モデムに接続されているASG上のネットワークカードのIPアドレスをここに入力します。このアドレスはモデムと同じサブネット内にある必要があります。例:`10.0.0.140`(AonSpeed)。

NICネットマスク(NIC Netmask): 使用するネットワークマスクをここに入力します。例:`255.255.255.0`(AonSpeed)。

pingアドレス(Ping Address)(オプション):ICMP ping要求に応答するインターネット上のホストのIPアドレスを入力します。ASGと外部ネットワーク間の接続をテストするには、PPTPリンクの反対側ホストのIPアドレスを入力する必要があります。ご利用のISPのDNSサーバを使用することができます。ASGはこのホストにping要求を送信します。応答がない場合は、接続不良です。

MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトでは、1492バイトのMTUが【*DSL(PPPoA)*】インタフェースタイプに設定されています。

毎日の再接続(Daily Reconnect): 接続を終了および再開する時間を定義します。【*無し(Never)*】を選択するか、具体的な時間を指定することができます。

再接続遅延(Reconnect Delay): ここで、再接続遅延を変更できます。デフォルトでは、遅延は【*5秒(5 Seconds)*】に設定されています。ご利用のISPがこれより長い遅延を要求している場合は、【*1分(One Minute)*】や【*15分(Fifteen Minutes)*】に設定できます。

非対称(Asymmetric)(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(Displayed Max)(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***【保存(Save)】*をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

5. **インタフェースを有効にします。**

   インタフェースを有効にするには、ステータスアイコンをクリックします。

   これでインタフェースが有効になります(ステータスアイコンは緑色)。まだインタフェースが*【ダウン(Down)】*と表示されている場合もあります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*【アップ(Up)】*メッセージが表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.9モデム(PPP)

設定するためには、ASGにシリアルインタフェースと外部PPPモデムが必要です。また、ユーザ名とパスワードを含むDSLアクセスデータも必要です。これらのデータは、インターネットサービスプロバイダ(ISP)から入手できます。

*モデム(PPP)*インタフェースを設定するには、次の手順に従ってください。

1. ***【インタフェース(Interfaces)】*タブで、*【新規インタフェース(New Interface)】*をクリックします。**
   *【新規インタフェースの作成(Create New Interface)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): インタフェースを説明する名前を入力します。

   タイプ(Type): ドロップダウンリストから*【モデム(PPP)(Modem(PPP))】*を選択します。

   ハードウェア(Hardware): ドロップダウンリストからインタフェースを選択します。

   IPv4デフォルトGW(IPv4 Default GW)(オプション):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   ユーザ名(Username): ISPが提供したユーザ名を入力します。

パスワード(Password): ISPが提供したパスワードを入力します。

ダイヤル文字列(Dial String): 電話番号を入力します。例: `5551230`

コメント(Comment)(オプション):説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
回線速度(Line Speed):ASGとモデムの間の接続に対して、速度をbps単位で設定します。一般的な値は57,600 bpsと115,200 bpsです。

フローコントロール(Flow Control): データフローをコントロールする方法を選択します。データがシリアル接続経由で転送される場合、システムで受信データを十分に速く処理できない可能性があります。データの損失が発生しないようにするためには、データフローのコントロール方法が必要になります。シリアル接続では、次の2つの方法を使用できます。

- *ハードウェア*信号
- *ソフトウェア*信号

PPP接続では、すべての8ビットがデータ転送回線に使用され、転送されるデータにはコマンドサイン*Control S*と*Control Q*のバイトが含まれるため、デフォルト設定の【*ハードウェア(Hardware)*】を維持し、シリアル接続ケーブルを使用することをお勧めします。

初期化文字列(Init String): モデムを初期化するための文字列を入力します。モデムに応じて初期化文字列の調整が必要になる可能性があります。この場合、初期化文字列は該当モデムのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

リセット文字列(Reset String): モデムのリセット文字列を入力します。モデムに応じてリセット文字列の調整が必要になる可能性があります。この場合、リセット文字列は該当モデムのマニュアルで確認できます。必要なマニュアルがない場合、デフォルト設定の*ATZ*を維持してください。

MTU: インタフェースの最大伝送単位をバイト単位で入力します。トラフィックマネジメントを使用する場合は、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して妥当な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズは、通信事業者とネットワークカードでサポートされていることが必要です(例:ギガビットインタフェース)。デフォルトでは、1492バイトのMTUが【*モデム(PPP) Modem(PPP)*】インタフェースタイプに設定されています。

非対称(Asymmetric)(オプション):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させたいときは、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切なユニットを選択します。

表示する最大(Displayed Max)(オプション):ダッシュボードに反映させたい場合は、ここに接続の最大ダウンリンク帯域幅を入力できます。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切なユニットを選択します。

4. ***【保存(Save)】をクリックします。***
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

5. **インタフェースを有効にします。**

   インタフェースを有効にするには、ステータスアイコンをクリックします。

   これでインタフェースが有効になります(ステータスアイコンは緑色)。まだインタフェースが*【ダウン(Down)】*と表示されている場合もあります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*【アップ(Up)】*メッセージが表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.2追加アドレス

1つのネットワークカードで追加IPアドレス(別名「*エイリアス*」)を設定できます。この機能を使用すると、1つの物理ネットワークカード上で複数の論理ネットワークを管理することができます。また、これを使用して、NAT(ネットワークアドレス変換)を実行しているASGにさらなるアドレスを割り当てることもできます。

標準イーサネットインタフェースで追加アドレスを設定するには、次の手順に従ってください。

1. ***【追加アドレス(Additional Addresses)】タブで、【新規追加アドレス(New Additional Address)】をクリックします。***
*【新規追加アドレスの作成(Create New Additional Address)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
名前(Name): 新しい追加アドレスを説明する名前を入力してください。

インタフェース(On Interface): アドレスを割り当てるインタフェースをドロップダウンリストから選択します。

IPv4アドレス(IPv4 Address): インタフェースのIPアドレスを入力します。

ネットマスク(Netmask): ドロップダウンリストからネットマスクを選択するか、IPv6ネットマスクを入力します(あるいはその両方)。

> **注 -** インタフェースを設定して、IPv4およびIPv6アドレスを同時に使用することができます。

コメント(Comment)(オプション): 説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(ステータスアイコンは赤色)。

4. **追加アドレスを有効にします。**
   追加アドレスを有効にするには、ステータスアイコンをクリックします。

   これで追加アドレスが有効になります(ステータスアイコンは緑)。追加アドレスはまだ「ダウン(*Down*)」と表示されている場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「アップ(*Up*)」というメッセージが表示されると、追加アドレスは完全に機能するようになっています。

追加アドレスを編集または削除するには、対応するボタンをクリックします。

6.1.3リンクアグリゲーション

リンクアグリゲーションは、「ポートトランキング」または「NICボンディング」とも呼ばれ、これによって複数のイーサネットネットワークポートを1つの仮想インタフェースに集約することができます。集約されたポートはシステム上で1つのIPアドレスとして表示されます。リンクアグリゲーションは、どの単体NICよりもリンク速度を向上させたり、いずれかのポートまたはスイッチで障害が発生した場合に冗長性を維持して基本フェイルオーバーおよびフォールトトレランス機能を提供したりするために役に立ちます。障害が発生したポートやスイッチにルーティングされているすべてのトラフィックは自動的にリルートされ、残りのポートまたはスイッチのいずれかを使用するようになります。このフェイルオーバーは、接続を使用しているシステムに対して完全に透過的です。

> **注 -** HA環境では、イーサネット接続を別のHAユニット上にすることもできます。

グループあたり最大4つのイーサネットインタフェースを使用して、リンクアグリゲーショングループを最大4つまで定義することができます。1つのリンクアグリゲーショングループには、少なくとも2つの空きネットワークインタフェースカードが必要です。そのうち1つは設定しないでください。

リンクアグリゲーショングループ(LAG)を作成するには、次の手順に従います。

1. **各LAGに対して、設定されたインタフェースを1つ選択します。**
   【*インタフェースの変換(Convert Interface)*】ドロップダウンリストから、リンクアグリゲーショングループに変換するインタフェースを選択します。

2. **各LAGに対して、設定されていないインタフェースを1つ選択します。**
   リンクアグリゲーショングループに追加するそれぞれの未設定インタフェースのチェックボックスにチェックを入れます。

3. **LAGを有効にします。**
   【*このグループを有効化(Enable this group)*】ボタンをクリックして、グループを有効にします。

   リンクアグリゲーショングループを設定すると、【*インタフェース(Interfaces)*】タブでインタフェース定義を作成するときに、新しいLAGインタフェース(`lag0`など)を選択できるようになります。ボンディングインタフェースの上部で、次のいずれかを作成できます。

   - イーサネット標準
   - イーサネットVLAN
   - ケーブルモデム (DHCP)
   - エイリアスインタフェース

LAGを無効にするには、LAGを構成するインタフェースのチェックボックスのチェックを外して、【*このグループを更新(Update this Group)*】をクリックします。LAGインタフェースのステータスが、【*サポート(Support)*】>>【*詳細(Advanced)*】>>【*インタフェーステーブル(Interfaces Table)*】タブに表示されます。

6.1.4アップリンクバランシング

アップリンクバランシング機能を使用すると、複数のインターネットアップリンクを組み合わせて、バックアップ用アップリンクを使用可能にするか、複数のアップリンクに負荷を分散することができます。組み合わせることができるアップリンクは最大8つです。

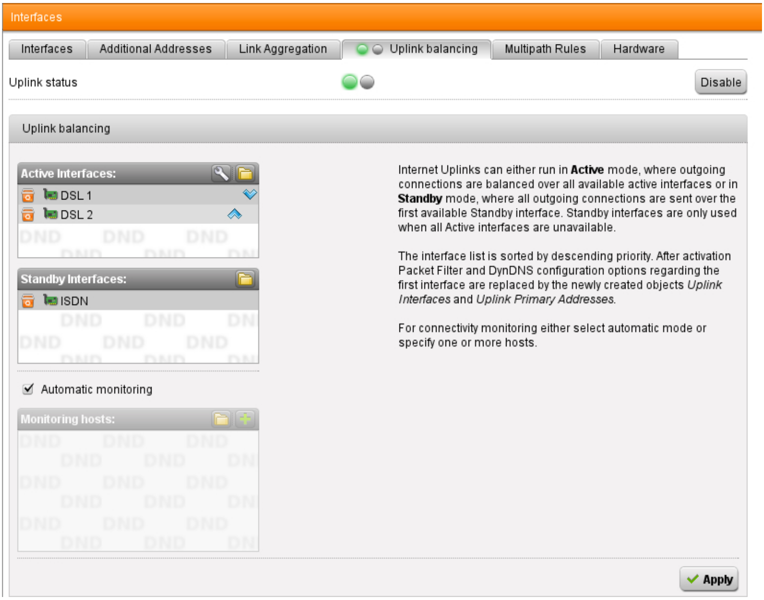


図47　インタフェース(Interfaces):アップリンクバランシングの設定

アップリンクバランシングを使用するには、次の手順に従ってください。

1. **アップリンクバランシングを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色になり、【*アップリンクバランシング(Uplink Balancing)*】エリアが編集可能になります。

2. **アクティブインタフェースを選択します。**
   フォルダアイコンをクリックしてインタフェースを1つ以上追加し、オブジェクトリストからインタフェースをドラッグします。複数のインタフェースがあれば、これらのインタフェースのトラフィックは自動的にバランシング(分散)されます。いずれかのインタフェースを使用できない場合、トラフィックは残りのインタフェースによってテイクオーバーされます。

   注 - アクティブインタフェースとスタンバイインタフェースの両方で、インタフェースの順序は重要な意味を持ちます。応答しないサーバがあると、このインタフェースの次のインタフェースが選択されます。インタフェースの順序は、該当ボックスで青色の矢印をクリックして変更します。

ボックスのヘッダで【スケジューラ(Scheduler)】ボタンを使用すると、個々のバランシング動作およびアクティブインタフェースのインタフェースパーシスタンスを設定することができます。

加重(Weight): 加重とは、あるインタフェースが処理するトラフィック量を他のインタフェースに対して相対的に示すもので、0～100の間で設定できます。加重ラウンドロビンアルゴリズムが使用され、値が大きいほど、該当インタフェースにルーティングされるトラフィックが多くなります。相対的な値であるため、合計して100にする必要はありません。たとえば、インタフェース1の値を100に、インタフェース2の値を50に、インタフェース3の値を0に設定することなどができます。この場合、インタフェース2のトラフィック量はインタフェース1の半分となり、インタフェース3は他のインタフェースが使用可能でない場合にのみ使用されます。0の値は、より値が大きい他のインタフェースが常に使用されることを示します(他のインタフェースが使用可能であれば)。

パーシスタンス(Itf. Persistence:): インタフェースパーシスタンスとは、クライアントからの後続の接続が常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間です。

3. **スタンバイインタフェースの選択(Select standby interfaces)**(オプション)
   ここでは、すべてのアクティブインタフェースが使用不能になった場合にのみ使用されるフェイルオーバーインタフェースをオプションで追加することができます。

   注 - アクティブインタフェースとスタンバイインタフェースをあわせて最大32件まで定義できます。

4. **モニタリングの有効化(Enable monitoring)**(オプション)
   デフォルトでは、インタフェース障害の可能性を検出するために【*自動モニタリング(Automatic Monitoring)*】が有効になっています。つまり、すべてのアップリンクバランシングインタフェースからインターネット上の任意のホストに15秒間隔でpingを実行することにより、それらのインタフェースの状態(健全性)がモニタリングされます。ホストがpingに応答しなくなった場合、そのインタフェースは機能していない(デッド(dead)である)と見なされるため、それ以降配信に使用されません。
   サーバプールを用いpingの対象とするホストを、ユーザが自分で定義することができます。

   1. **【*自動モニタリング(Automatic Monitoring)*】チェックボックスからチェックを外します。**
      【*モニタリングホスト(Monitoring Hosts)*】ボックスが編集可能になります。

2. **pingの対象となるホストを追加します。**
任意のホストを使用する代わりにpingの対象としたいホストを、1つ以上選択または追加します。

5. ***【適用(Apply)】*をクリックします。**
設定が保存されます。

*「アップリンクインタフェース(Uplink Interfaces)」*という名前の新しい仮想ネットワークインタフェースが自動的に作成され、Astaro Security Gatewayの他の機能(IPsecルールなど)で使用できるようになっています。仮想ネットワークインタフェース*「アップリンクインタフェース(Uplink Interfaces)」*は、インタフェースリストに追加されたすべてのアップリンクインタフェースから構成されています。
さらに、*「アップリンクプライマリアドレス(Uplink Primary Addresses)」*という名前の新しいネットワークグループが自動的に作成され、Astaro Security Gatewayの他の機能(ファイアウォールルールなど)で使用できるようになっています。これは、すべての*アップリンクインタフェース*のプライマリアドレスを参照します。

DynDNSが使用されている場合や、リモートサーバがすべてのアップリンクインタフェースのIPアドレスを受け付けることができる場合は、インタフェースで障害が発生したときに、次に使用可能なインタフェースを介してオープンなVPNトンネルを自動的に再確立することができます。前提条件としては、IPsecルールが*【ローカルインタフェース(Local Interface)】*として*【アップリンクインタフェース(Uplink Interfaces)】*を使用する必要があります。

6.1.5マルチパスルール

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【インタフェース(Interfaces)】>>【マルチパスルール(Multipath Rules)】*タブでは、アップリンクバランシング用のルールを設定できます。このルールは*【アップリンクバランシング(Uplink Balancing)】*タブでアクティブインタフェースに適用されます。すべてのアクティブインタフェースに障害が発生し、パッシブインタフェースがテイクオーバーすると、マルチパスルールはパッシブインタフェースに適用されます。もちろんルールは、トラフィックのバランシング(分散)を行うべき複数のインタフェース(アクティブまたはパッシブ)がある場合にのみ適用されます。一般にすべてのサービスは、マルチパスルールを作成する必要なくバランシングされます。ただし、マルチパスルールを使用すると、特定のトラフィックのバランシングを追加で定義することができます。

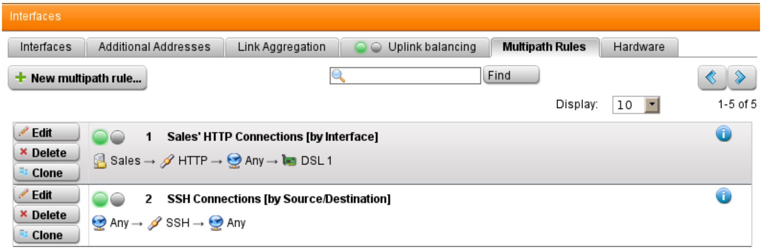


図48 インタフェース(Interfaces):マルチパスルール

マルチパスルールを作成するには、次の手順に従います。

1. **【マルチパスルール(Multipath Rules)】タブで、【新規マルチパスルール(New Multipath Rule)】をクリックします。**
   *【新規マルチパスルールの作成(Create New Multipath Rule)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): マルチパスルールを説明する名前を入力してください。

   送信元(Source): 照合する送信元IPアドレスまたはネットワークを選択または追加します。

   サービス(Service): 照合するネットワークサービスを選択または追加します。

   宛先(Destination): ルーティングに使用すべき宛先IPアドレスまたはネットワークを選択または追加します。

   インタフェース パーシスタンス(Itf. Persistence:): *インタフェースパーシスタンス*とは、クライアントからの後続の接続が常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間です。何を基準にパーシスタンスを定めるかを定義することができます。

   - **接続毎(By Connection)**: それぞれの接続は個別にバランシングされます。
   - **送信元毎(By Source)(デフォルト)**: バランシングは、送信元IPアドレスに基づいて行われます。
   - **宛先毎(By Destination)**: バランシングは、宛先IPアドレスに基づいて行われます。
   - **送信元/宛先毎(By Source/Destination)**: バランシングは、送信元/宛先IPアドレスの組み合わせに基づいて行われます。

- **インタフェース毎(By Interface)**:【*バインドインタフェース(Bind Interface)*】ドロップダウンリストからインタフェースを選択します。ルールに該当するすべてのトラフィックは、このインタフェース経由でルーティングされます。インタフェースで障害が発生し、照合ルールが他にない場合、接続はデフォルトの動作にフォールバックします。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
新しいマルチパスルールが【*マルチパスルール(Multipath Rules)*】リストに追加されます。ルールを編集または削除するには、対応するボタンをクリックします。

4. **ルールを有効にします。**
新しいマルチパスルールはデフォルトで無効になっています。ルールを有効にするには、ステータスアイコンをクリックします。

   これでルールが有効になります(ステータスアイコンは緑)。

6.1.6ハードウェア

【*インタフェースおよびルーティング(Interfaces & Routing)*】>>【*インタフェース(Interfaces)*】>>【*ハードウェア(Hardware)*】タブには、設定されているすべてのインタフェースが、イーサネットオペレーションモード、MACアドレスなどの情報と共に表示されます。各インタフェースに対し、オートネゴシエーションを有効または無効にすることができます。

オートネゴシエーション(Autonegotiation): 通常、2つのネットワークデバイス間のイーサネットオペレーションモード(10BASE-T全二重、10BASE-T半二重など)が自動的にネゴシエーションされ、これらのデバイスで共有される最適なオペレーションモードが選択されます。このとき、速度は高速(100 Mbps)の方が低速(10 Mbps)より優先され、同じ速度では全二重の方が半二重より優先されます。

イーサネットオペレーションモードの手動での選択がドライバでサポートされていないネットワークインタフェースカードや、対応する設定を決定できないネットワークインタフェースカードのために、オートネゴシエーションはデフォルトで有効になっています。そのため、オートネゴシエーションはVMwareインストールなどに対して有効にします。

オートネゴシエーション設定を変更するには、各インタフェースカードの【*編集(Edit)*】ボタンをクリックし、【*リンクモード(Link Mode)*】のドロップダウンリスト経由で、表示される【*NICパラメータの編集(Edit NIC Parameters)*】ダイアログウィンドウで設定を変更します。【*保存(Save)*】をクリックして変更を保存します。

警告 - オートネゴシエーションを無効にするときは注意してください。これにより、不一致が生じ、パフォーマンスが大幅に低下したり、接続が切断したりする可能性もあります。該当するネットワークインタフェースカードがWebAdminへのインタフェースである場合、WebAdminへのアクセスが切断されてしまいます。

HAリンクモニタリング(HA Link Monitoring): 冗長化が有効である場合、設定されたすべてのインタフェースでリンクステータスがモニタリングされます。リンクに障害が発生した場合、テイクオーバーが引き起こされます。設定されたインタフェースが常に接続されている訳ではない場合(管理インタフェースなど)、このインタフェースのHAリンクモニタリングは無効にしてください。無効にしないと、すべてのHAリンクのステータスが「未リンク(UNLINKED)」のままになります。HAリンクモニタリングを無効にするには、各インタフェースカードの【*編集(Edit)*】ボタンをクリックして、表示される【*NICパラメータの編集(Edit NIC Parameters)*】ダイアログウィンドウで設定を変更します。【*保存(Save)*】をクリックして変更を保存します。

仮想MACの設定(Set Virtual MAC): デバイスのMACアドレスを変更できると便利な場合があります。たとえば、ISPによっては、モデムに接続されているデバイスに変更があった場合にこのモデムをリセットし、デバイスのMACアドレスをリセットする必要があります。MACアドレスを前のデバイスの値に設定することで、モデムのリセットを回避することができます。

ただし、ASGはデバイスのオリジナルのMACアドレスを上書きするのではなく、仮想MACアドレスを設定します。これを行うには、該当するインタフェースカードの【*編集(Edit)*】ボタンをクリックします。表示される【*NICパラメータの編集(Edit NIC Parameters)*】ダイアログウィンドウで、【*仮想MACの設定(Set Virtual MAC)*】チェックボックスにチェックを入れ、有効なMACアドレスを入力します。【*保存(Save)*】をクリックして変更を保存します。

オリジナルのMACアドレスに復元するには、該当するインタフェースカードの【*編集(Edit)*】ボタンをクリックします。表示される【*NICパラメータの編集(Edit NIC Parameters)*】ダイアログウィンドウで、【*仮想MACの設定(Set Virtual MAC)*】チェックボックスのチェックを外します。【*保存(Save)*】をクリックして変更を保存します。

6.2ブリッジング

ブリッジングとは、主にイーサネットネットワークで使用されるパケット転送技術です。ルーティングと違い、ブリッジングでは特定のアドレスがネットワーク内のどこにあるのか推定するのではなく、ブロードキャスティングを使用して不明のデバイスを探します。

ブリッジングにより、複数のイーサネットネットワークまたはセグメントが相互接続できるようになります。データパケットはブリッジングテーブルを介して転送されます。ブリッジングテーブルは、ブリッジ

ポートにMACアドレスを割り当てます。作成されるブリッジは、ブリッジインタフェースを介してトラフィックを透過的に受け渡します。

注 - このようなトラフィックは、適切なファイアウォールルールによって明示的に許可する必要があります。

6.2.1 ステータス

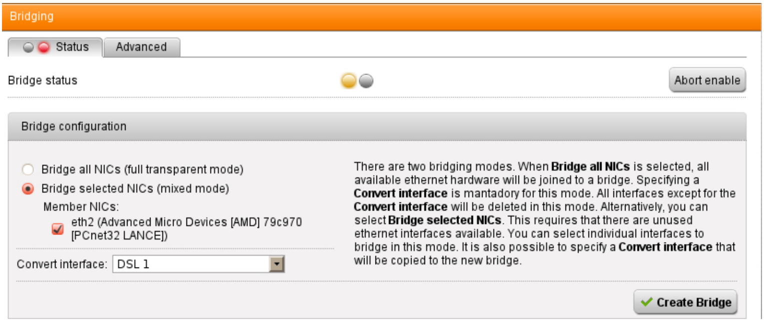


図49 ブリッジ:ブリッジの設定

ブリッジを設定するには、次の手順に従ってください。

1. ***【ステータス(Status)】タブでブリッジを有効にします。***
   *【インタフェースおよびルーティング(Interfaces & Routing)】>>【ブリッジ(Bridging)】>>【ステータス(Status)】*タブで、ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【ブリッジ設定(Bridge Configuration)】*エリアが編集可能になります。

2. **ブリッジングモードを選択します。**
   2種類のモードから選択可能です。

   - **全NICをブリッジ(Bridge all NICs)**: このオプションを選択すると、使用可能なすべてのイーサネットNIC(ネットワークインタフェースカード)がブリッジに加わります。このモードでは*【変換インタフェース(Convert Interface)】*の指定が必須となります。変換されたインタフェースを除くすべてのインタフェースが削除されます。

   - **選択したNICをブリッジ(Bridge Selected NICs)**: ブリッジを形成する個々のNICを選択できます。このためには、使用されていないネットワークインタフェース

カードを用意する必要があります。使用されていないネットワークインタフェースカードを1つ以上選択してブリッジを形成します。また、新しいブリッジにコピーされる変換インタフェースを指定することもできます。

3. **ブリッジに変換されるインタフェースを選択します。**
   設定済みのインタフェースのみを選択できます。ブリッジは、そのインタフェースのアドレス設定と、エイリアスアドレスおよびVLANの設定を継承します。

4. ***【ブリッジの作成(Create Bridge)】をクリックします。***
   ネットワークインタフェースが組み合わされ、ブリッジがアクティブになります(ステータスアイコンが緑色になります)。

設定をキャンセルするには、*【有効化を中止(Abort Enable)】*またはアンバー色のステータスアイコンをクリックします。

ブリッジの設定が完了すると、*【インタフェースおよびルーティング(Interfaces & Routing)】>>【インタフェース(Interfaces)】*タブに、変換されたインタフェースがSysID `br0`のブリッジデバイスとして表示されます。ブリッジのメンバであるすべてのインタフェースが*【ブリッジ設定(Bridge Configuration)】*エリアに表示されます。ブリッジからインタフェースを除外するには、チェックボックスからチェックを外して、*【ブリッジの更新(Update Bridge)】*をクリックします。

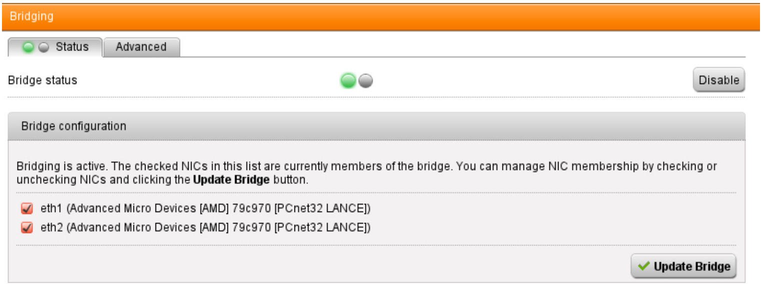


図50 ブリッジ:ブリッジングが有効

ブリッジを削除するには、次の手順に従ってください。

1. ***【ステータス(Status)】タブで、【無効(Disable)】をクリックします。***
   ステータスアイコンがアンバー色になります。

2. ***【ブリッジの削除を確認(Confirm Removal of Bridge)】をクリックします。***
   ステータスアイコンが赤色に変わります。ブリッジは正常に削除されました。

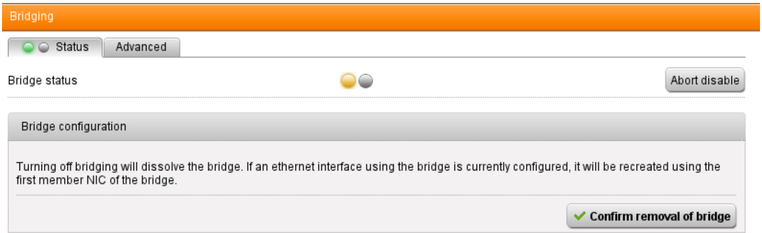


図51　ブリッジ：ブリッジを無効にする

6.2.2詳細

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【ブリッジ(Bridging)】>>【詳細(Advanced)】*タブでは、次のブリッジオプションを設定できます。

ARPブロードキャストを許可(Allow ARP broadcasts)：この機能を使用すると、グローバルARPブロードキャストをブリッジで転送するかどうかを設定することができます。有効にすると、ブリッジはMAC宛先アドレス`FF:FF:FF:FF:FF:FF`へのブロードキャストを許可します。ただし、これは疑わしい攻撃者に悪用され、各ネットワークセグメント内に導入されているネットワークカードや、場合によってはセキュリティ製品自体について、さまざまな情報を収集するために利用されてしまう危険性があります。そのため、デフォルト設定はこのようなブロードキャストがブリッジを通過できないようになっています。

時間経過タイムアウト(Ageing Timeout)：この時間(秒)が経過すると、無効なMACアドレスが削除されます。デフォルト時間は300秒です。

IPv6パススルーを許可(Allow IPv6 Pass Through)：このオプションを有効にすると、IPv6トラフィックが検査を受けずにブリッジを通過できるようになります。

6.3スタティックルーティング

ネットワークに接続されたすべてのコンピュータは、ルーティングテーブルを使用して、発信したデータパケットを宛先に届くように送信するためのパスを決定します。たとえば、ルーティングテーブルには、宛先アドレスがローカルネットワーク上にあるか、またはデータパケットをルータに転送するべきかどうか、といった情報が含まれています。ルータを使用する場合は、テーブルには、どのルータをどのネットワークに使用するかという情報が含まれます。

Astaro Security Gatewayのルーティングテーブルには、標準スタティックルートとポリシルートという2種類のルートを追加できます。スタティックルートでは、ルーティングターゲットはパケットの宛先

アドレスだけで決定されます。ポリシルートでは、送信元インタフェース、送信元アドレス、サービス、あるいは宛先アドレスに基づいてルーティングを決定できます。

注： -ゲートウェイのインタフェースに接続されたネットワークに対して、追加ルートを設定する必要はありません。また、デフォルトルートも設定する必要はありません。これらのルートはシステムが自動的に追加します。

6.3.1 標準スタティックルート

システムに直接接続されたネットワークについては、システムがルーティングエントリをルーティングテーブルに自動的に挿入します。特定ネットワーク経由でアクセスする追加ルータを使用する場合は、エントリを手動で入力する必要があります。直接接続されていないネットワークへのルートで、コマンドまたは設定ファイルを使ってルーティングテーブルに挿入されるものをスタティックルートと呼んでいます。

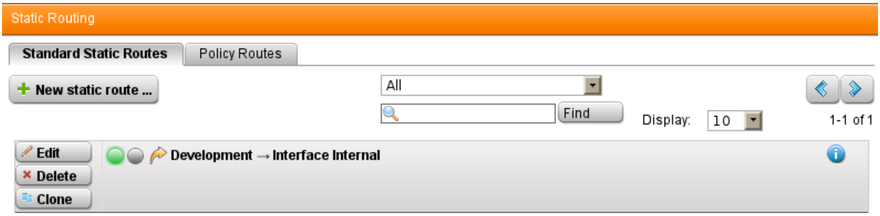


図52 スタティックルーティング：スタティックルートテーブル

標準スタティックルートを追加するには、以下の手順に従います。

1. ***【新規スタティックルート(New Static Route)】をクリックします。***
   *【新規スタティックルートを作成(Create New Static Route)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ルートタイプ(Route Type)：次のルートタイプを使用できます。

   - **インタフェースルート(Interface Route)**：パケットは特定のインタフェースで送出されます。これは2つの状況で役立ちます。1番目は、ダイナミック(動的)インタフェース上のルーティング(PPP)の場合です。この理由は、この場合はゲートウェイのIPアドレスが不明だからです。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。

- **ゲートウェイルート(Gateway Route)**: パケットは特定のホスト(ゲートウェイ)に送信されます。
- **ブラックホールルート(Blackhole Route)**: パケットは確認なしで廃棄されます。これはOSPF または他のダイナミックアダプティブ(動的適応型の)ルーティングプロトコルでルーティングループやルートフラッピングなどを回避する場合に役に立ちます。

ネットワーク(Network):ゲートウェイがインターセプトするデータパケットの宛先ネットワークを選択します。

インタフェース(Interface): データパケットがゲートウェイを離れるインタフェースを選択します(ルートタイプとして【*インタフェースルート(Interface Route)*】を選択した場合のみ利用できます)。

ゲートウェイ(Gateway):ゲートウェイがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプとして【*ゲートウェイルート(Gateway Route)*】を選択した場合のみ利用できます)。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   新しいルートが【*標準スタティックルート(Standard Static Route)*】リストに表示されます。
4. **ルートを有効にします。**
   ルートを有効にするには、ステータスアイコンをクリックします。

ルートを編集または削除するには、対応するボタンをクリックします。

6.3.2ポリシルート

ルータがデータパケットを受信すると、通常はパケットの宛先アドレスに基づいて転送先を決定し、この宛先アドレスを使用してルーティングテーブルのエントリが検索されます。ただし、他の基準に基づいてパケットを転送することが必要な場合もあります。ポリシベースのルーティングでは、お客様のポリシに従ってデータパケットをフォワーディング(転送)またはルーティングできます。

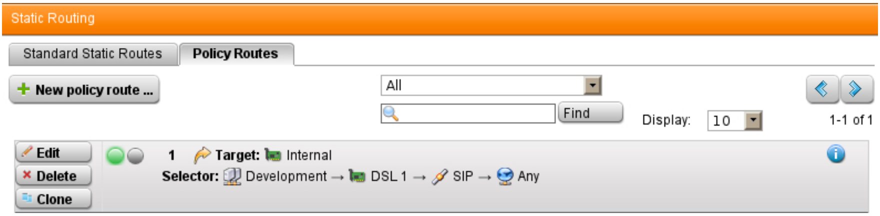


図53 スタティックルーティング:ポリシルートテーブル

ポリシルートを追加するには、以下の手順に従います。

1. ***【新規ポリシルート(New Policy Route)】をクリックします。***
   *【新規ポリシルートを作成(Create New Policy Route)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   位置(Position): 位置番号。これによってポリシルートの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルートは昇順に照合されます。あるルートが一致すると、それ以降、それより大きい番号のルートは評価されません。

   ルートタイプ(Route Type): 次のルートタイプを使用できます。

   - **インタフェースルート(Interface Route)**: パケットは特定のインタフェースで送出されます。これは2つの状況で役立ちます。1番目は、ダイナミック(動的)インタフェース上のルーティング(PPP)の場合です。この理由は、この場合はゲートウェイのIPアドレスが不明だからです。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。

   - **ゲートウェイルート(Gateway Route)**: パケットは特定のホスト(ゲートウェイ)に送信されます。

   送信元インタフェース(Source Interface): ルーティングされるデータパケットが到着したインタフェース。*【すべて(Any)】*を設定すると、すべてのインタフェースが該当することになります。

   送信元ネットワーク(Source Network): ルーティングされるデータパケットの送信元ネットワーク。*【すべて(Any)】*を設定すると、すべてのネットワークが該当することになります。

   サービス(Service): ルーティングされるデータパケットに一致するサービス定義。ドロップダウンリストには、定義済みのサービスとお客様が定義されたサービスがすべて含まれます。これらのサービスにより、どのようなトラフィックを処理するかを精密に指定できます。*【すべて(Any)】*を設定すると、プロトコル、送信元、および宛先ポートのあらゆる組み合わせに一致します。

宛先ネットワーク(Destination Network): ルーティングされるデータパケットの宛先ネットワーク。【*すべて(Any)*】を設定すると、すべてのネットワークが該当することになります。

ターゲットインタフェース(Target Interface): データパケットの送信先インタフェース(ルートタイプとして【*インタフェースルート(Interface Route)*】を選択したときのみ使用可能)。

ゲートウェイ(Gateway): ゲートウェイがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに【*ゲートウェイルート(Gateway Route)*】を選択した場合のみ使用可能)。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいルートが【*ポリシルート(Policy Routes)*】リストに表示されます。

4. **ルートを有効にします。**
   ルートを有効にするには、ステータスアイコンをクリックします。

ルートを編集または削除するには、対応するボタンをクリックします。

6.4ダイナミックルーティング(OSPF)

OSPF(Open Shortest Path First)プロトコルは、リンクステート型の階層ルーティングプロトコルであり、大規模な自律システム(AS)ネットワーク内で主に使用されます。Astaro Security Gateway はOSPFバージョン2をサポートしています。他のルーティングプロトコルと比べ、OSPFはルーティングメトリックとしてコストを使用しています。OSPF対応インタフェースのコストは、特定のインタフェース経由でパケットを送信するときに必要なオーバーヘッドを示します。インタフェースのコストは、そのインタフェースの帯域幅に反比例します。そのため、帯域幅が大きいと、コストが小さくなります。たとえば、10 Mbpsのイーサネット回線より56 Kbpsのシリアル回線の方がオーバーヘッドが増え(コストが高くなり)、遅延時間が長くなります。

接続されたネットワークのコストの計算方法は、OSPF仕様には指定されておらず、ベンダーに任されています。そのため、独自の計算式を定義することができます。ただし、コストがすでに定義されている他のネットワークとOSPFネットワークが隣接している場合、同じ計算ベースを適用することをお勧めします。

デフォルトでは、インタフェースのコストは帯域幅に基づいて計算されます。たとえば、Ciscoの場合、10^8をインタフェースの帯域幅(bps)で割ってコストを計算しています。この計算式を使用すると、10 Mbpsのイーサネット回線を経由する場合のコストは10^8/10000000 = 10となりま

す。一方、1.544 Mbpsの回線(T1)では、$10^8/1544000 = 64$となります(コストの計算では、小数点以下を切り捨てます)。

6.4.1 グローバル

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【ダイナミックルーティング(OSPF)(Dynamic Routing(OSPF))】>>【グローバル(Global)】*タブでは、OSPFの基本設定を行うことができます。OSPF機能を有効にする前に、OSPFエリアを1つ以上設定しておく必要があります(*【エリア(Area)】*タブ)。

警告 - Astaro Security GatewayのOSPF機能を設定するためには、OSPFプロトコルを熟知している技術的に熟練した経験豊富な管理者が必要です。ここでの設定オプションについての解説は、OSPFプロトコルについて完全に理解するために十分であるとは言えません。そのため、この機能は慎重に使用することをお勧めします。設定を誤ると、ネットワークが動作不可能になる場合があります。

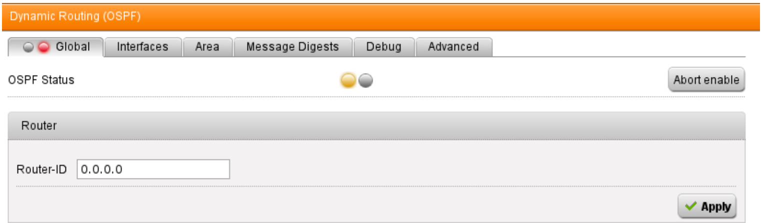


図54　OSPF：OSPFの有効化

OSPFを設定するには、次の手順に従ってください。

1. ***【エリア(Area)】*タブで、OSPFエリアを1つ以上作成します。**
2. ***【グローバル(Global)】*タブで、OSPFを有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、【ルータ(Router)】エリアが編集可能になります。
3. **ルータIDを入力します。**
   Astaro Security Gatewayデバイスを他のOSPFルータから識別するための一意のルータIDを入力します。
4. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

OSPFを無効にするには、ステータスアイコンまたは*【無効(Disable)】*をクリックします。

6.4.2エリア

OSPFネットワークは、複数のエリアに分割されます。エリアとは、ネットワークの残りの部分のために情報をひとまとめにできるルータの論理グループです。エリアの識別名は、10進ドット表記の32ビットIDであり、IPアドレスの表記法と似ています。

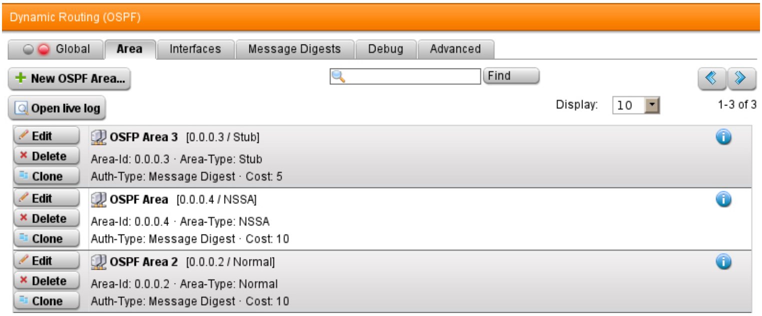


図55 OSPF:設定されたエリアの概要

OSPFエリアは全部で6種類あります。

- **バックボーン**: IDが0(または`0.0.0.0`)のエリアはOSPFネットワークバックボーンに予約されており、OSPFネットワークの中核となります。他のすべてのエリアがこのエリアに接続されます。

- **通常(Normal)**: ノーマルエリア(または標準エリア)は、1(または`0.0.0.1`)~4,294,967,295(または`255.255.255.255`)という一意のID範囲を持ちます。ノーマルエリアは、ABR(*エリア境界ルータ*)を介して外部ルートを双方向的にフラッディングして処理します。外部ルートとは、他のルーティングプロトコルからOSPF内に配布されたルートとして定義されます。

- **スタブ(Stub)**: 通常、スタブエリアは外部ネットワークと直接接続されません。外部ネットワークへのすべてのトラフィックはABR(*エリア境界ルータ*)を介してルーティングする必要があるため、スタブエリアに外部ルートをインジェクトする必要はありません。そのため、スタブエリアは外部ネットワークにトラフィックを送信する外部ルートにとってデフォルトルートの代わりとなります。

- **スタブサマリなし(Stub No-Summary)**: *スタブサマリなしエリア(Stub No-Summary)*または完全*スタブエリア(totally stubby area)*はスタブエリアと似ていますが、このエリアはいわゆるサマリルートを許可しません。つまり、タイプ3のサマリリンクステートアドバタイズメント(LSA)を拒絶し、エリアに入ってこないようにします。

- **NSSA**: NSSA(not-so-stubby area)は、スタブエリアとは違い、外部接続をサポートできます。NSSAはバーチャルリンクをサポートしない点に注意が必要です。
- **NSSAサマリなし(NSSA No-Summary)**: *NSSAサマリなし(NSSA No-Summary)*はNSSAと似ていますが、このエリアはいわゆるサマリルートを許可しません。つまり、タイプ3のサマリリンクステートアドバタイズメント(LSA)を拒絶し、エリアに入ってこないようにします。

OSPFエリアを作成するには、次の手順に従います。

1. ***【エリア(Area)】タブで、【新規OSPFエリア(New OSPF Area)】をクリックします。***
   *【新規OSPFエリアの作成(Create New OSPF Area)】*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name): エリアを説明する名前を入力してください。

   エリアID(Area ID): エリアのIDを10進ドット表記で入力します(たとえばノーマルエリアは`0.0.0.1`、バックボーンエリアは`0.0.0.0`)。

   エリアタイプ(Area Type): エリアタイプ(説明は前述)を選択し、該当するエリアに割り当てられるネットワークの特徴を指定します。

   認証タイプ(Auth-Type): エリア内のインタフェースを介して送受信されるすべてのOSPFパケットに対して使用する認証タイプを選択します。次の認証タイプを使用できます。

   - **MD5**: 選択すると、MD5認証が有効になります。MD5(Message-Digest algorithm 5)とは、128ビットのハッシュ値を使用する一般的な暗号ハッシュ関数です。
   - **プレーンテキスト(Plain-Text)**: 選択すると、プレーンテキスト認証が有効になります。パスワードはネットワーク上を平文の形で伝送されます。
   - **オフ(Off)**: 選択すると、認証が無効になります。

   インタフェース経由で接続(Connect Via Interface): OSPF対応インタフェースを選択します。ここでOSPF対応インタフェースを指定するためには、事前に*【インタフェース(Interfaces)】*タブでこのインタフェースを作成しておく必要があります。

   バーチャルリンクを使用(Connect Virtual Links): OSPF*自律システム*(AS)内のすべてのエリアは、バックボーンエリア(エリア0)に物理的に接続されている必要があります。物理的な接続が不可能な場合には、バーチャルリンクを使用して、非バックボーンエリアを介してバックボーンに接続できます。*【仮想リンクの接続(Connect Virtual Links)】*ボックスに、バーチャルリンクのネイバーに関連付けられたルータIDを10進ドット表記で入力します(`10.0.0.8`など)。

コスト(Cost): このエリアでデータパケットを送受信するコスト。有効な値は1～65535の範囲内です。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
新しいエリア定義が*【エリア(Area)】*タブに表示されます。

OSPFエリアを編集または削除するには、対応するボタンをクリックします。

ライブログを開く(Open Live Log): OSPFライブログには、OSPFインタフェースでのすべてのアクティビティが記録されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

6.4.3インタフェース

【ネットワークおよびルーティング(Interfaces & Routing)】>>*【ダイナミックルーティング(OSPF)(Dynamic Routing(OSPF))】*>>*【インタフェース(Interfaces)】*タブでは、OSPFエリア内で使用するインタフェースの定義を作成できます。それぞれの定義には、OSPF対応インタフェースに固有の複数のパラメータがあります。

OSPFインタフェース定義を作成するには、次の手順に従います。

1. ***【インタフェース(Interfaces)】タブで、【新規OSPFインタフェース(New OSPF Interface)】をクリックします。***
*【新規OSPFインタフェースの作成(Create New OSPF Interface)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
名前(Name): このインタフェースを説明する名前を入力してください。

インタフェース(Interface): このOSPFインタフェース定義と関連付けるインタフェースを選択します。

認証タイプ(Auth-Type): このインタフェースを介して送受信されるすべてのOSPFパケットに対して使用する認証タイプを選択します。次の認証タイプを使用できます。

- **MD5**: 選択すると、MD5認証が有効になります。MD5(Message-Digest algorithm 5)とは、128ビットのハッシュ値を使用する一般的な暗号ハッシュ関数です。

- **プレーンテキスト(Plain-Text)**: 選択すると、プレーンテキスト認証が有効になります。パスワードはネットワーク上を平文の形で伝送されます。

- **オフ(Off)**: 選択すると、認証が無効になります。

メッセージダイジェスト(Message Digest): このOSPFインタフェースに対してMD5認証が使用されることを示すメッセージダイジェスト(MD)を選択します。ここでメッセージダイジェストを選択するためには、事前に【*メッセージダイジェスト(Message Digests)*】タブでそのメッセージダイジェストを作成しておく必要があります。

コスト(Cost): このインタフェースでデータパケットを送信するコスト。有効な値は1～65535の範囲内です。

詳細オプション(Advanced Options)(オプション):【*詳細オプション(Advanced Options)*】チェックボックスにチェックを入れると、追加の設定オプションが表示されます。

- **Hello間隔(Hello Interval)**:Astaro Security Gatewayがこのインタフェースを介して*Hello*パケットを送信する間隔(秒)を指定します。デフォルト値は10秒です。
- **再送間隔(Retransmit Interval)**: LSA(リンクステートアドバタイズメント)を受け取ったという確認応答のACKがインタフェースに届かなかったときに、インタフェースがLSAを再送する間隔(秒)を指定します。デフォルト値は5秒です。
- **Dead間隔(Dead Interval)**:Astaro Security Gatewayがこのインタフェースを介して*Hello*パケットの受信を待機する期間(秒)を指定します。デフォルト値は40秒です。原則的に、*Dead間隔*の値は*Hello間隔*の値の4倍の長さにします。
- **優先順位(Priority)**: ルータの優先順位を1～255の範囲の8ビット値で指定します。この値は、特定のネットワークの指名ルータ(DR)を決定するために主に使用されます。デフォルト値は1です。
- **送信遅延(Transmit Delay)**: インタフェースでLSU(link state update)パケット送信に予想される期間(秒)を指定します。範囲は1～65535秒で、デフォルト値は1です。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
   OSPFインタフェース定義が【*インタフェース(Interfaces)*】タブに表示されます。

OSPFインタフェースを編集または削除するには、対応するボタンをクリックします。

ライブログを開く(Open Live Log): OSPFライブログには、OSPFインタフェースでのすべてのアクティビティが記録されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

6.4.4メッセージダイジェスト

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【メッセージダイジェスト(Message Digests)】*タブでは、いわゆるメッセージダイジェスト鍵を生成することができます。メッセージダイジェスト鍵は、OSPFでMD5認証を有効にするために必要です。MD5認証では、パスワードを使用してメッセージダイジェストを生成します。これはデータパケットとパスワードの128ビットのチェックサムです。メッセージダイジェストは、パスワードと関連付けられた鍵IDとともにデータパケットで送信されます。

注 - 受信側ルータは、同じメッセージダイジェスト鍵で設定されていなければなりません。

メッセージダイジェスト鍵を作成するには、次の手順に従います。

1. ***【メッセージダイジェスト(Message Digest)】*タブで*【新規メッセージダイジェスト鍵(New Message Digest Key)】*をクリックします。**
   *【新規メッセージダイジェスト鍵の作成(Create New Message Digest Key)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ID: このメッセージダイジェスト鍵の鍵IDを入力します。範囲は1～255です。

   MD5鍵(MD5-key): 関連するパスワードを入力します。最大16文字の英数字から成る文字列にする必要があります。

3. ***【保存(Save)】*をクリックします。**
   新しい鍵が*【メッセージダイジェスト(Message Digests)】*リストに表示されます。

ダイジェスト鍵を編集または削除するには、対応するボタンをクリックします。

6.4.5デバッグ

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【ダイナミックルーティング(OSPF)(Dynamic Routing(OSPF))】>>【デバッグ(Debug)】*タブでは、関連OSPFパラメータについての詳細情報が別のブラウザウィンドウで表示されます。次の情報が含まれています。

- **OSPFネイバの表示(Show IP OSPF Neighbor)**: OSPFネイバ情報をインタフェース単位で表示するために使用します。

- **OSPFルートの表示(Show IP OSPF Routes)**: ルーティングテーブルの現在の状態を表示するために使用します。
- **OSPFインタフェースの表示(Show IP OSPF Interface)**: OSPF関連のインタフェース情報を表示するために使用します。
- **OSPFデータベースの表示(Show IP OSPF Database)**: 特定ルータのOSPFデータベースに関連する情報を一覧表示するために使用します。
- **OSPF境界ルータの表示(Show IP OSPF Border-Routers)**: ABR*(エリア境界ルータ)*とASBR*(自律システム境界ルータ)*への内部OSPFルーティングテーブルのエントリを表示するために使用します。

6.4.6詳細

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【ダイナミックルーティング(OSPF)(Dynamic Routing(OSPF))】>>【詳細(Advanced)】*タブには、OSPFに関連する追加の設定オプションがあります。これらは、OSPF以外のドメインからOSPFドメインへのルーティング情報の再配布に関連するものです。

注 - ポリシルートを再分配することはできません。

直接接続されたネットワークを再配布(Redistribute Connected): 直接接続されているネットワークのルートを再配布する場合は、これを選択します。デフォルトのメトリック(コスト)値は10です。

スタティックルートを再配布(Redistribute Static): スタティックルートおよびIPsecルートを再分配する場合は、これを選択します。デフォルトのメトリック(コスト)値は10です。

注 - IPsecトンネルを再配分するためにはストリクトルーティングを無効化する必要があります(「接続」)。

デフォルトルートを配布(Announce Default Route): デフォルトルートをOSPFドメインに再配布する場合は、これを選択します。

注 - デフォルトルートは、`0.0.0.0/0`へのルートの有無を問わずOSPFドメインにアドバタイズされます。

リンク検出(Link Detection): インタフェースリンクが検出された場合にのみインタフェースのルートをアナウンスする場合は、これを選択します。

6.5IPv6

バージョン8から、Astaro Security Gateway はIPv4の後継であるPv6をサポートしています。

管理ガイドの以下の機能は、IPv6を完全にまたは部分的にサポートします。

- WebAdminおよびユーザポータルへのアクセス
- SSH
- NTP
- SNMP
- インタフェースタイプ: イーサネット標準、PPPoE、イーサネットVLAN、(ケーブルモデム/Dhclient限定)
- DNS
- DHCPサーバ
- IPS
- ファイアウォール
- ICMP
- Webフィルタ
- SMTP
- IPsec(サイト間のみ)
- Syslogサーバ

6.5.1グローバル

【*IPv6*】>>【*グローバル(Global)*】タブでは、Astaro Security GatewayのIPv6サポートを有効にすることができます。さらに、これを有効にすると、IPv6の情報(ステータス情報など)がここに表示されます。

IPv6サポートはデフォルトでは無効になっています。IPv6を有効にするには、次の手順に従います。

1. **【*グローバル(Global)*】タブで、IPv6を有効化します。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

ステータスアイコンが緑色に変わります。以前にIPv6を有効化または設定したことがない場合は、*【接続(Connectivity)】*エリアに*【なし(None)】*と表示されます。

IPv6を有効にすると、複数のネットワークや、WebAdminでIPv6を明示的に参照しているその他のオブジェクト定義が表示されます。これらは、IPv4オブジェクトと同様に使用することができます。

注 - IPv6を有効にすると、ネットワークオブジェクトなどのアイコンに、該当オブジェクトがIPv6オブジェクトかIPv4オブジェクトか(あるいはその両方か)を示すマークが追加で表示されます。

6.5.2プレフィックス通知

*【IPv6】>>【プレフィックス通知(Prefix Advertisement)】*タブでは、Astaro Security Gatewayを設定して、クライアントにIPv6アドレスプレフィックスを割り当てて、クライアントが自力でIPv6アドレスを選択できるように設定することができます。プレフィックス通知(またはルータアドバタイズメント)とは、IPv6の機能の1つであり、ルータ(この場合管理ガイド)がIPv4におけるDHCPサーバと同じように機能します。ただし、ルータはクライアントにIPを直接割り当てません。代わりに、IPv6ネットワーク内のクライアントは、ルータとのプライマリ通信のためにいわゆるリンクローカルアドレスを自らに割り当てます。続いて、ルータがクライアントにネットワークセグメントのプレフィックスを伝えます。その後、クライアントはプレフィックスと自らのMACアドレスから成るIPアドレスを生成します。

新しいプレフィックスを作成するには、次の手順に従います。

1. ***【プレフィックス通知(Prefix Advertisement)】タブで、【新規プレフィックス(New Prefix)】をクリックします。***
   *【新規プレフィックスの作成(Create New Prefix)】*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   インタフェース(Interface): 64 ビットのネットマスクが設定されたIPv6アドレスを持つインタフェースを選択します。

   DNSサーバ1/2(DNS Server 1/2)(オプション):DNSサーバのIPv6アドレス。

   ドメイン(Domain)(オプション):クライアントに送信されるドメイン名を入力します(例:`intranet.example.com`)。

   有効期間(Valid Lifetime): プレフィックスが有効となる期間。デフォルトは30日間です。

推奨期間(Preferred Lifetime): この期間を超過すると、推奨されるライフタイムがまだ満了していない他のプレフィックスがクライアントに選択されます。デフォルトは7日間です。

Other configurationフラグ(Other config)(オプション):このオプションはデフォルトで選択されています。これにより、所与のプレフィックスに対して所与のDNSサーバとドメイン名がDHCPv6経由で追加でアナウンスされます。現時点では、プレフィックスアドバタイズメントからDNS情報をフェッチできるクライアントは少ないため、この機能が役に立つます(RFC 5006/ RFC 6106)。このDHCPv6設定は非表示であり、DHCP設定メニューでの表示や編集はできません。このオプションは、IPv6をWindows Vista/7環境で使用するためには必須です。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
新しいプレフィックス設定が*【プレフィックス通知(Prefix Advertisements)】*リストに表示されます。

6.5.36to4

【IPv6】>>*【6to4】*タブでは、既存のIPv4ネットワーク上でIPv6アドレスを自動的にトンネリングするようにAstaro Security Gatewayを設定することができます。6to4を使用すると、各IPv4アドレスに、マッピング先のIPv6ネットワークから`/48`プレフィックスが付加されます。生成されるIPv6アドレスは、プレフィックス`2002`と16進表記のIPv4アドレスから構成されます。

注 - *【6to4】*を有効にするか*【トンネルブローカ(Tunnel Broker)】*を使用するかのいずれかを選択できます。

特定のインタフェースのIPアドレストンネリングを有効にするには、次の手順に従います。

1. ***【6to4】*タブで6to4を有効化します。**
ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【6to4】*エリアと*【詳細(Advanced)】*エリアが編集可能になります。

2. **インタフェースを選択します。**
*【インタフェース(Interfaces)】*ドロップダウンリストから、パブリックIPv6アドレスが設定されているインタフェースを選択します。

3. **【適用(Apply)】をクリックします。**
設定が保存されます。インタフェースステータスは【*グローバル(Global)*】タブに表示されます。

詳細

【*サーバアドレス(Server Address)*】を変更して、別の6to4リレーサーバを使用することができます。

設定を保存するには【*適用(Apply)*】をクリックします。

6.5.4トンネルブローカ

【*IPv6*】>>【*トンネルブローカ(Tunnel Broker)*】タブでは、トンネルブローカの使用を有効にすることができます。トンネルブローカは一部のISPが提供するサービスであり、これを利用するとIPv6アドレスを使用してインターネットにアクセスできます。

注 -【*6to4*】を有効にするか【*トンネルブローカ(Tunnel Broker)*】を使用するかのいずれかを選択できます。

Astaro Security Gateway は、次のトンネルブローカをサポートします。

- Teredo(匿名のみ)
- Freenet6(GoGo6)(匿名またはユーザアカウント使用)
- SixXS(ユーザアカウントが必要)

トンネルブローカを使用するには、次の手順に従います。

1. **【トンネルブローカ(Tunnel Broker)】タブで、トンネルブローカの使用を有効にします。**
ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンが緑色になり、【*トンネルブローカ(Tunnel Broker)*】エリアと【*詳細(Advanced)*】エリアが編集可能になります。Teredoの匿名認証を使用すると、トンネルブローカはすぐに有効になります。接続ステータスは【*グローバル(Global)*】タブに表示されます。

トンネルブローカ

デフォルトのトンネルブローカ設定を変更できます。

認証(Authentication): ドロップダウンリストから認証方法を選択します。

- **匿名(Anonymous)**: この方法を使用すると、各ブローカにユーザアカウントを指定する必要はありません。割り当てられるIPアドレスは一時的なものです。
- **ユーザ(User)**: 各ブローカに登録して、ユーザアカウントを取得する必要があります。

ブローカ(Broker): ドロップダウンリストから他のブローカを選択できます。

ユーザ名(Username)(*【ユーザ(User)】*のみで使用可能): 各ブローカにユーザ名を指定します。

パスワード(Password)(*【ユーザ(User)】*のみで使用可能): ユーザ名のパスワードを入力します。

設定を保存するには*【適用(Apply)】*をクリックします。

詳細

ここでは、選択したトンネルブローカに対して他のサーバアドレスを指定できます。

設定を保存するには*【適用(Apply)】*をクリックします。

6.6サービス品質(QoS)

一般的に、*サービス品質*(QoS)とは、選択されたネットワークトラフィックにより良いサービスを提供する制御メカニズムを示し、特に、保証された帯域幅という点で優先することを意味します。Astaro Security Gatewayでは、優先トラフィックは、*【サービス品質(QoS)(Quality of Service(QoS))】*タブで設定します。この設定では、ネットワークの2点間を通過する特定タイプの送信ネットワークトラフィックに対し、保証された帯域幅を確保できますが、一方で、受信トラフィックのシェーピングはSFQ(*確率的不偏キューイング(Stochastic Fairness Queuing)*)あるいはRED(*ランダム初期検知(Random Early Detection)*)などのさまざまなテクニックによって内部的に最適化されます。

6.6.1ステータス

【サービス品質(QoS)(Quality of Service(QoS))】>>*【ステータス(Status)】*タブには、QoSを設定できるインタフェースがリストされます。デフォルトでは、QoSは各インタフェースに対して無効になっています。

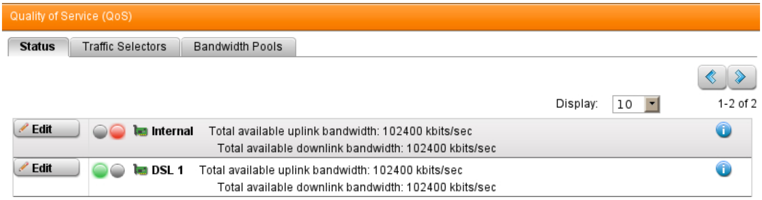


図56 QoS:【ステータス(Status)】ページ

各インタフェースについて、*【編集(Edit)】*をクリックして、ISPが提供したアップリンクおよびダウンリンク帯域幅(Kbps)を設定します。たとえば、アップリンクとダウンリンクの両方に5Mビット/秒(Mbps)のインターネット接続を設定するには、「5120」と入力します。

帯域幅が変動する場合は、ISPが保証した最低の値を入力します。たとえば、アップリンクとダウンリンクの両方に0.8Mビット/秒(Mbps)の変動のある5Mビット/秒(Mbps)のインターネット接続を使用する場合は、4300Kビット/秒(Kbps)と入力します。利用できる帯域幅が一時的に設定した最低保証値より高くなると、ゲートウェイは新しい帯域幅を考慮して予想して、優先トラフィックの帯域幅のパーセンテージが同様に高くなるようにしますが、これは残念ながら、その反対には作用しません。

アップリンクを制限(Limit Uplink): このオプションを選択すると、QoS機能は、設定されたダウンリンクとアップリンクの帯域幅を、このインタフェースを通過するトラフィックを優先順位付けするための計算ベースとして使用します。デフォルトでは*【アップリンクを制限(Limit Uplink)】*オプションは選択されており、以下のインタフェースタイプに使用されます。

- 標準イーサネットインタフェース(ゲートウェイとインターネット間にルータが配備され、ルータが提供する帯域幅がわかっているもの)
- イーサネットVLAN インタフェース(ゲートウェイとインターネット間にルータが配備され、ルータが提供する帯域幅がわかっているもの)
- DSL (PPPoE)
- DSL(PPPoA)
- モデム(PPP)

トラフィックシェーピングの計算ベースがインタフェースの最大速度で決定されるインタフェースの*【アップリンクを制限(Limit Uplink)】*チェックボックスからチェックを外します。ただし、これは以下のインタフェースタイプにのみ適用されます。

- 標準イーサネットインタフェース(インターネットに直接接続)
- イーサネットVLANインタフェース(インターネットに直接接続)
- ケーブルモデム(DHCP)

特定のアップリンク制限が指定されていないインタフェースでは、QoS機能が全トラフィックを均等にシェーピングします。たとえば、ケーブルモデムインタフェース上のVoIPトラフィックに512Kビット/秒(Kbps)を設定した場合に、利用できる帯域幅が半分になったときは、256Kビット/秒がこのトラフィックに使用されます(比例シェーピングは、固定最大制限に依存するインタフェースと対照的に、双方向に機能することに注意してください)。

ダウンロードイコライザ(Download Equalizer): 有効にすると、*確率的不偏キューイング*(SFQ)および*ランダム初期検知*(RED)キューアルゴリズムがネットワークの輻輳を回避します。設定したダウンリンク速度に達すると、ストリームを使用するほとんどのダウンリンクのパケットはドロップします。

アップロードオプティマイザ(Upload Optimizer): 有効にすると、送信TCP接続の確立(*SYN*フラグが設定されたTCPパケット)、TCP接続のACK(確認応答)パケット(*ACK*フラグが設定され、パケット長が40～60バイトのTCPパケット)、およびDNS ルックアップ(UDP53上のUDPパケット)が自動的に優先されます。

6.6.2トラフィックセレクタ

トラフィックセレクタは、QoSが扱う特定タイプのネットワークトラフィックを記述したQoS の定義と見なすことができます。これらの定義は、後で帯域幅プール定義の中で使用されます。帯域幅プール定義では、帯域幅全体の制限や特定量の最低帯域幅の保証など、QoSによるこのトラフィックの取り扱い方法について定義できます。

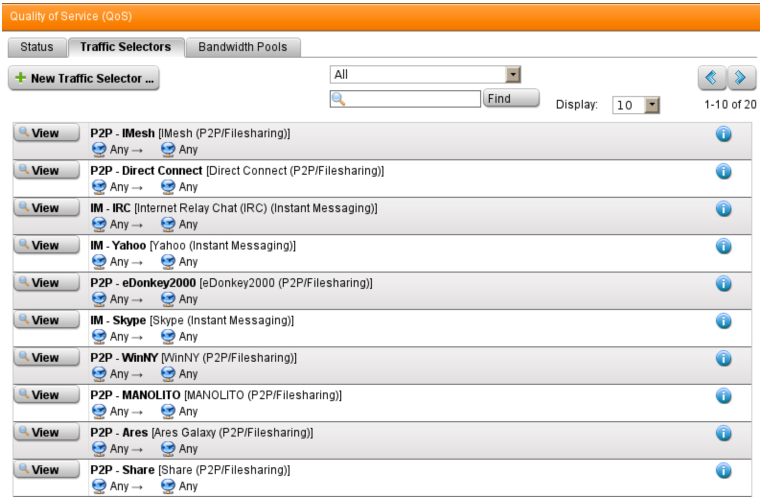


図57　QoS:トラフィックセレクタ

トラフィックセレクタを作成するには、以下の手順に従います。

1. ***【トラフィックセレクタ(Traffic Selector)】タブで、【新規トラフィックセレクタ(New Traffic Selector)】をクリックします。***
   *【新規トラフィックセレクタの作成(Create New Traffic Selector)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): このトラフィックセレクタを説明する名前を入力します。

   セレクタタイプ(Selector Type): 以下のタイプを定義できます。

   - **トラフィックセレクタ(Traffic Selector)**: トラフィックセレクタを使用すると、トラフィックは1つのサービスまたはサービスグループに基づいてシェーピングされます。
   - **アプリケーションセレクタ(Application Selector)**: アプリケーションセレクタを使用すると、トラフィックはアプリケーションに基づいてシェーピングされます。つまり、使用するポートやサービスを問わず、どのトラフィックがどのアプリケーションに属しているかに基づきます。
   - **グループ(Group)**: 複数のサービスおよびアプリケーションセレクタを1つのトラフィックセレクタルールにまとめることができます。グループを定義するには、単体のセレクタをいくつか定義している必要があります。

   送信元(Source): QoSを有効にする送信元ネットワークを選択します。

サービス(Service):*トラフィックセレクタのみ。*QoSを有効にするネットワークサービスを選択します。事前に定義したさまざまなサービスやサービスグループから選択できます。たとえば、固定帯域幅をVoIP接続に予約する場合は、VoIP プロトコル(SIP およびH.323および H.323)を選択します。

宛先(Destination): QoSを有効にする宛先ネットワークを選択します。

TOS/DSCP:*トラフィックセレクタのみ。*IPヘッダの*TOS/DSCP*フィールドを使用して優先トラフィックをマークするには、これを選択します。たとえば、大規模なVoIPのインストールで、TOS/DSCP フラグはVoIPトラフィックをマークするためによく使用されます。VoIPプロトコルに基づいたVoIP接続に固定帯域幅を予約しない場合は、VoIP環境内で使用されるTOSビットあるいはDSCPビットを選択します。

- **TOSビット(TOS-bits)**: TOS(サービスタイプ)ビットを選択する場合は、以下の設定から選択できます。
  - 通常のサービス(Normal service)
  - 費用を最小化(Minimize monetary cost)
  - 信頼性を最大化(Maximize reliability)
  - スループットを最大化(Maximize throughput)
  - 遅延を最小化(Minimize delay)
- **DSCPビット(DSCP-bits)**: DSCPビット(差別化サービスコードポイント)を選択する場合は、単一の【*DSCP値(DSCP Value)*】(0～63の整数)を指定するか、または【*DSCPクラス(DSCP Class)*】リストから事前に定義した値を選択できます(例:*BE default dscp (000000)*)。

コントロール基準(Control By):*アプリケーションセレクタのみ。*アプリケーションタイプに基づいてトラフィックをシェーピングするか、分類に基づくダイナミックフィルタによってコントロールするかを選択します。

- **アプリケーション(Applications)**: トラフィックは、アプリケーションに基づいてシェーピングされます。【*コントロール対象のアプリケーション(Control These Applications)*】ボックスでアプリケーションを1つ以上選択します。
- **ダイナミックフィルタ(Dynamic Filter)**: トラフィックは、分類に基づいてシェーピングされます。【*コントロール対象の分類(アプリケーション)*】ボックスで分類を1つ以上選択します。

コントロール対象のアプリケーション/分類(Control These Applications/Categories):*アプリケーションセレクタのみ。*フォルダアイコンをクリックし

て、アプリケーション/分類を選択します。ダイアログウィンドウが開きます。これについては、次のセクションで詳しく説明します。

生産性(Productivity): *ダイナミックフィルタのみ*。選択した生産性スコアが反映されます。

リスク(Risk): *ダイナミックフィルタのみ*。選択したリスクスコアが反映されます。

注 - 一部のアプリケーションはシェーピングできません。これは、Astaro Security Gatewayの適切なオペレーションのために必要です。このようなアプリケーションは、【*アプリケーション選択(Select Application)*】ダイアログウィンドウのアプリケーションテーブルでチェックボックスがオフになっています。たとえば、*WebAdmin*、*Teredo*、*SixXs*(IPv6トラフィック用)、*Portal*(ユーザポータルのトラフィック用)などが該当します。ダイナミックフィルタを使用すると、これらのアプリケーションのシェーピングも自動的に制限されます。

コメント(Comment)(オプション): 説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
新しいセレクタが【*トラフィックセレクタ(Traffic Selectors)*】リストに表示されます。

多くのトラフィックセレクタを定義した場合は、1つのトラフィックセレクタグループに複数のセレクタをまとめることで、より便利に使用することが可能になります。

このトラフィックセレクタまたはトラフィックセレクタグループは、それぞれの帯域幅プールで使用できます。これらのプールは【*帯域幅プール(Bandwidth Pools)*】タブで定義できます。

【アプリケーションまたはカテゴリの選択(Select Application or Category)】ダイアログウィンドウ

アプリケーションコントロールルールを作成する際は、【*コントロール対象のアプリケーション/カテゴリを1つ以上選択(Select one or more Applications/Categories to control)*】というダイアログウィンドウからアプリケーションまたはアプリケーションカテゴリを選択する必要があります。

ダイアログウィンドウの下部に表示されるテーブルには、選択可能なアプリケーションまたは定義したカテゴリに属するアプリケーションが表示されます。デフォルトでは、すべてのアプリケーションが表示されます。

ダイアログウィンドウの上部には、テーブルに表示されるアプリケーション数を制限するための3つの設定オプションがあります。

- **Category(カテゴリ)**: アプリケーションはカテゴリ別にグループ分けされています。このリストには、利用可能なすべてのカテゴリが表示されます。デフォルトでは、すべてのカテゴリが

選択されています。つまり、下部に表示されるテーブルには、利用可能なすべてのアプリケーションが表示されます。表示されるアプリケーションを特定のカテゴリに絞り込むには、クリックしてカテゴリリストを開き、1つ以上のカテゴリを選択します。

- **生産性(Productivity)**: アプリケーションは、生産性への影響(つまり生産性にこのアプリケーションが与える影響の度合い)によっても分類されています。例:一般的なビジネスソフトウェアのSalesforceのスコアは5です。つまり、これを使用することで生産性が向上します。一方、オンラインゲームのFarmvilleのスコアは1で、これを使用すると生産性が低下します。ネットワークサービスDNSのスコアは3で、生産性への影響は中立的です。
- **リスク(Risk)**: アプリケーションは、使用時のリスク(マルウェア、ウイルス感染、攻撃)によっても分類されています。数値が高いほど、リスクも高くなります。

ヒント - それぞれのアプリケーションには情報アイコンがあり、クリックすると各アプリケーションの説明が表示されます。テーブルヘッダの検索ボックスを使用して、テーブル内を検索することができます。

次に、【*新規トラフィックセレクタの作成(Create New Traffic Selector)*】ダイアログウィンドウで選択したコントロールのタイプに応じて、以下を行います。

- ダイナミックフィルタでコントロールする場合:【*適用(Apply)*】をクリックして、選択したアプリケーションをルールに適用します。
- アプリケーションでコントロールする場合:テーブルで、アプリケーションの前のチェックボックスをクリックし、コントロール対象のアプリケーションを選択します。【*適用(Apply)*】をクリックして、選択したアプリケーションをルールに適用します。

【*適用(Apply)*】をクリックするとダイアログウィンドウが閉じ、トラフィックセレクタルールの設定の編集を続けることができます。

6.6.3帯域幅プール

【*サービス品質(Quality of Service)*】>>【*帯域幅プール(Bandwidth Pools)*】タブで、帯域幅を管理するための帯域幅プールを定義して管理できます。

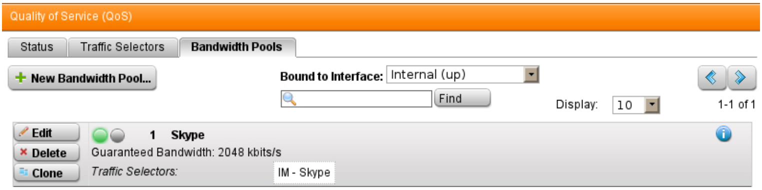


図58 QoS:帯域幅プール

帯域幅プールを作成するには、以下の手順に従います。

1. ***【帯域幅プール(Bandwidth Pools)】タブで、インタフェースを選択します。***
   ドロップダウンリストから、帯域幅プールを作成するインタフェースを選択します。

2. ***【新規帯域幅プール(New Bandwidth Pool)】をクリックします。***
   【新規帯域幅プールの作成(*Create New Bandwidth Pool*)】ダイアログボックスが開きます。

3. **次の設定を行います。**
   名前(Name): この帯域幅プールを説明する名前を入力します。

   位置(Position): 位置番号。これによって帯域幅プールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。帯域幅プールは昇順に照合されます。ある帯域幅プールが一致すると、それ以降、それより大きい番号の帯域幅プールは評価されません。より具体的な帯域幅プールをリストの上部に配置して、曖昧な帯域幅プールが最後に照合されるようにします。たとえば、一般的なWebトラフィック(HTTP)と特定ホストへのWebトラフィックにトラフィックセレクタを設定した場合は、帯域幅プールリストの最上部に後者のトラフィックセレクタを使用する帯域幅プールを配置します(つまり、位置1をそれに選択します)。この優先処理は、使用するトラフィックセレクタが異なるQoS対応インタフェースに割り当てられている場合は適用できません。

4. **帯域幅(Bandwidth)**: この帯域幅プール用に予約するアップリンク帯域幅をKビット単位で入力します。たとえば、特定タイプのトラフィックに1Mビット/秒(Mbps)を予約する場合は、`1024`と入力します。

   > **注 -** 帯域幅プールに割り当てられるのは、利用可能な全帯域幅の90 %までです。ゲートウェイは常に帯域幅の10 %をいわゆるシェーピングされていないトラフィック用に予約します。上記の例で言えば、アップリンクのインターネット接続が5Mビット/秒(Mbps)で、VoIPトラフィックにできるだけ多くの帯域幅を割り当てたい場合は、最大4608Kビット/秒(Kbps)を入力できます。

帯域幅の上限を指定(Specify Upper Bandwidth Limit): 上記の【*帯域幅(Bandwidth)*】フィールドに入力した値は、特定の種類のトラフィック用に予約される保証された帯域幅を示します。しかし、帯域幅プールは通常、可能であれば、そのトラフィック用により多くの帯域幅を割り当てます。特定のトラフィックが一定量以上の帯域幅を使用しないようにしたい場合は、このオプションを選択して、この帯域幅プールによって使用される帯域幅の割り当てを上限値に制限します。

トラフィックセレクタ(Traffic Selector): この帯域幅プールに使用するトラフィックセレクタを選択します。

コメント(Comment)(オプション):説明などの情報を追加します。

5. ***【保存(Save)】をクリックします。***
   新しい帯域幅プールが【*帯域幅プール(Bandwidth Pools)*】リストに表示されます。

6.7マルチキャストルーティング(PIM-SM)

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【マルチキャストルーティング(PIM-SM)(Multicast Routing(PIM-SM))】*メニューを使用すると、ネットワーク上で使用するPIM-SM*(Protocol Independent Multicast Sparse Mode)*を設定することができます。PIMとは、複数ネットワーク内でマルチキャストパッケージを動的(ダイナミック)にルーティングするためのプロトコルです。マルチキャストとは、複数のクライアントが受信するパッケージをできるだけ小さいトラフィックを使用して効率的に配信するための技術です。通常、複数のクライアント宛てのパケットは、コピーされて各クライアントに個別に送信されるため、消費される帯域幅はユーザ数に応じて増大します。そのため、同じパッケージを同時に要求する多数のクライアントを抱えるサーバ(コンテンツのストリーミング用サーバなど)の場合、大量の帯域幅が必要となります。

これに対しマルチキャストは、ネットワークの各リンク経由でパケットを一度だけ送信することにより帯域幅を節約します。これを実現するために、マルチキャストでは、サーバ(送信者)からクライアント(受信者)への経路上でいつコピーを作成するかを決定するために、適切に設定されたルータを使用します。これらのルータは、PIM-SMを使用してアクティブなマルチキャスト受信者を追跡し、ルーティングの設定にこの情報を使用します。

PIM-SM通信の簡単な説明は次のようになります。送信者がマルチキャストデータの送信を開始します。送信者用のマルチキャストルータがPIM-SM経由でRPルータに登録し、RPルータは送信者のルータにJoinメッセージを送信します。マルチキャストパケットが送信者からRPルータに流れるようになります。受信者が、このマルチキャストグループのIGMPブロードキャスト経由でローカ

ルPIM-SMルータに自己登録します。このルータは受信先用のJoin要求をRPルータに向けて送信し、RPルータはマルチキャストトラフィックを受信者に転送します。

マルチキャストは、独自のIPアドレス範囲(`224.0.0.0/4`)を持ちます。

6.7.1グローバル

*【マルチキャストルーティング(PIM-SM)(Multicast Routing(PIM-SM))】>>【グローバル(Global)】*タブでは、PIMを有効または無効にできます。*【ルーティングデーモンの設定(Routing Daemon Settings)】*エリアには、関与するインタフェースとルータのステータスが表示されます。

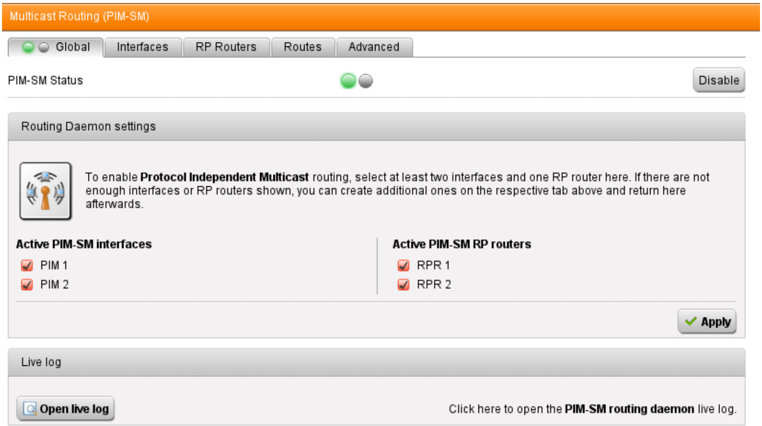


図59 PIM-SM:設定例

PIMを有効にする前に、*【インタフェース(Interfaces)】*タブでPIMインタフェースとして機能するインタフェースを2つ以上定義して、*【RPルータ(RP Routers)】*タブでルータを1台定義する必要があります。

PIM-SMを有効にするには、次の手順に従います。

1. ***【グローバル(Global)】*タブでPIM-SMを有効化します。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【ルーティングデーモンの設定(Routing Daemon Settings)】*が編集可能になります。

2. **次の設定を行います。**
   アクティブなPIM-SMインタフェース(Active PIM-SM Interfaces): PIM-SMに使用するインタフェースを2つ以上選択します。インタフェースの設定は【*インタフェース(Interfaces)*】タブで行います。

   アクティブなPIM-SM RPルータ(Active PIM-SM RP Routers): PIM-SMに使用するRPルータを1つ以上選択します。RPルータの定義は【*RPルータ(RP Routers)*】タブで行います。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。ネットワークでPIM-SM通信が有効になりました。

設定をキャンセルするには、【*有効化を中止(Abort Enable)*】またはアンバー色のステータスアイコンをクリックします。PIM-SMを無効にするには、ステータスアイコンまたは【*無効(Disable)*】ボタンをクリックします。

ライブログ

【*ライブログを開く(Open Live Log)*】ボタンをクリックすると、新しいウィンドウでPIMライブログが開きます。

6.7.2インタフェース

【*マルチキャストルーティング(PIM-SM)(Multicast Routing(PIM-SM))*】>>【*インタフェース(Interfaces)*】タブでは、どのAstaro Security Gatewayインタフェース上でマルチキャスト通信を行うかを定義することができます。

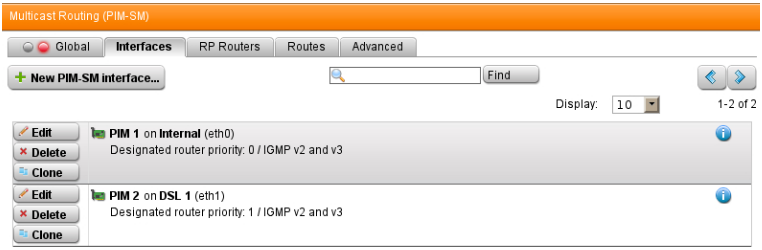


図60 PIM-SM:インタフェースリスト

新しいPIM-SMインタフェースを作成するには、次の手順に従います。

1. **【*インタフェース(Interfaces)*】タブで、【*新規PIM-SMインタフェース(New PIM-SM Interface)*】をクリックします。**

*【新規PIM-SMインタフェースの作成(New PIM-SM Interface)】*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   名前(Name): PIM-SMインタフェースを説明する名前を入力してください。

   インタフェース(Interface): PIMおよびIGMPネットワークトラフィックを許可するインタフェースを選択します。

   DR優先順位(DR priority)(オプション):インタフェースの指定ルータ(DR)の優先順位を定義する番号を入力します。同じネットワークセグメント内に複数のPIM-SMルータが存在する場合、優先順位が最も高いルータがIGMP要求を受け付けます。0～ 2^{32}までの数字を使用できます。優先順位を指定しないと、デフォルトで0が使用されます。

   IGMP: サポートするIGMP*(Internet Group Management Protocol)*のバージョンを選択します。IGMPは、受信者がマルチキャストグループのメンバシップを確立するために使用します。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいPIM-SMインタフェースがインタフェースリストに追加されます。

PIM-SMインタフェースを編集または削除するには、対応するボタンをクリックします。

6.7.3RPルータ

ネットワーク上でマルチキャストを使用できるようにするためには、1つ以上のランデブーポイントルータ(RPルータ)を設定する必要があります。RPルータは、マルチキャスト受信者と送信者の両方から登録を受け付けます。RPルータとは、特定のマルチキャストグループのRPルータとして選ばれた通常のPIM-SMルータでもあります。どのルータがRPルータとなるかについて、すべてのPIM-SMルータが合意する必要があります。

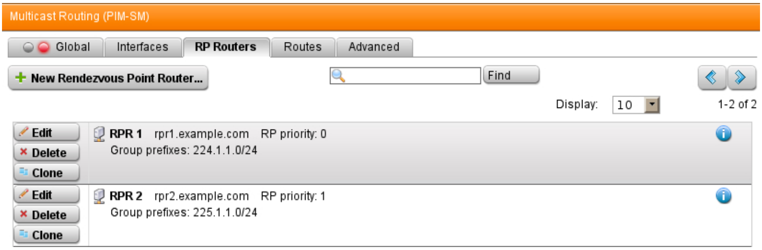


図61 PIM-SM:ランデブーポイントルータのリスト

RPルータを作成するには、次の手順に従います。

1. ***【RPルータ(RP Routers)】タブで【新規ランデブーポイントルータ(New Rendezvous Point Router)】をクリックします。***
   *【新規RPルータの作成(Create a New RP Router)】*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   名前(Name): RPルータを説明する名前を入力してください。

   ホスト(Host): RPルータとして機能するホストを作成(または選択)します。

   優先順位(Priority): RPルータの優先順位を定義する数字を入力します。優先順位が一番低いRPルータに、Joinメッセージが送信されます。`0`~`255`の数字を使用できます。優先順位を指定しないと、デフォルトで`0`が使用されます。

   マルチキャストグループのプレフィックス(Multicast Group Prefixes): RPルータが担当するマルチキャストグループを入力します。RPルータが複数のマルチキャストグループを担当する場合は、グループのプレフィックスを`224.1.1.0/24`のように定義できます。マルチキャストグループ(プレフィックス)は、マルチキャストアドレスの範囲内(`224.0.0.0/4`)にする必要があります。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   新しいRPルータがルータのリストに追加されます。

RPルータを編集または削除するには、対応するボタンをクリックします。

6.7.4ルート

受信者と送信者の間に、継続的な通信ルートをセットアップする必要があります。受信者、送信者、RPルータが同じネットワークセグメント内にない場合、これらの間の通信を可能にするルートを作成する必要があります。

図62 PIM-SM:ルートリスト

PIM-SMルートを作成するには、次の手順に従います。

1. ***【ルート(Routes)】タブで、【新規PIM-SMルート(New PIM-SM route)】をクリックします。***
   *【新規PIM-SMルートの作成(Create a New PIM-SM Route)】*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   ルートタイプ(Route Type): 次のルートタイプを使用できます。

   - **インタフェースルート(Interface Route)**: パケットは特定のインタフェースで送出されます。これは2つの状況で役立ちます。1番目は、ダイナミック(動的)インタフェース上のルーティング(PPP)の場合です。この理由は、この場合はゲートウェイのIPアドレスが不明だからです。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。

   - **ゲートウェイルート(Gateway Route)**: パケットは特定のホスト(ゲートウェイ)に送信されます。

   ネットワーク(Network): PIMトラフィックをルーティングする宛先アドレス範囲を選択します。

   ゲートウェイ(Gateway): ゲートウェイがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに*【ゲートウェイルート(Gateway Route)】*を選択した場合のみ使用可能)。

   インタフェース(Interface): ゲートウェイがデータパケットを転送するインタフェースを選択します(ルートタイプに*【インタフェースルート(Interface Route)】*を選択した場合のみ使用可能)。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   新しいPIM-SMルートがルートのリストに追加されます。

PIM-SMルートを編集または削除するには、対応するボタンをクリックします。

6.7.5詳細

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【マルチキャストルーティング(PIM-SM)(Multicast Routing(PIM-SM))】>>【詳細(Advanced)】*タブでは、PIMの詳細設定を構成することができます。

最短パスツリー設定(Shortest Path Tree Settings)

一部のネットワークでは、送信者、RP、受信者の間のPIM通信ルートは可能な限り最短のネットワークパスとはなりません。*【最短パスツリーへの切り替えを有効化(Enable Switch to Shortest Path Tree)】*オプションを使用すると、特定のトラフィックしきい値に達したときに送信者と受信者の間の既存の通信を最短パスに切り替えて、モデレータのRPを省くことができます。

自動ファイアウォール設定(Auto Firewall Settings)

このオプションを有効にすると、指定されたマルチキャストグループにマルチキャストトラフィックを転送するために必要となるすべてのファイアウォールルールがシステムによって自動的に作成されます。

デバッグ設定(Debug Settings)

PIM-SMルーティングデーモンログで追加のデバッグ情報を表示するには、*【デバッグモードを有効化(Enable Debug Mode)】*オプションを選択します。

6.8アップリンクモニタリング

*【インタフェースおよびルーティング(Interfaces & Routing)】>>【アップリンクモニタリング(Uplink Monitoring)】*メニューでは、アップリンク接続をモニタリング(監視)し、接続ステータスが変化したときに自動的に適用するアクションを定義することができます。

6.8.1グローバル

*【アップリンクモニタリング(Uplink Monitoring)】>>【グローバル(Global)】*タブで、アップリンクのモニタリングを有効または無効にできます。

アップリンクモニタリングを有効にするには、*【有効(Enable)】*ボタンまたはステータスアイコンをクリックします。
ステータスアイコンが緑色に変わります。*【アップリンクステータス(Uplink Status)】*セクションに、アップリンク接続が確立している場合は*【オンライン(ONLINE)】*、アップリンク接続がダウンしている

場合は【*オフライン(OFFLINE)*】と表示されます。設定をキャンセルするには、【*有効化を中止(Abort Enable)*】またはアンバー色のステータスアイコンをクリックします。

6.8.2アクション

【*インタフェースおよびルーティング(Interfaces & Routing)*】>>【*アップリンクモニタリング(Uplink Monitoring)*】>>【*アクション(Action)*】タブで、アップリンクの接続ステータスが変更になった場合に自動的に適用するアクションを定義できます。たとえば、アップリンク接続がダウンした場合は追加アドレスを無効にすることができます。

新しいアクションを作成するには、以下の手順に従います。

1. **【*アクション(Actions)*】タブで、【*新規アクション(New Action)*】をクリックします。**
   【*アップリンクオフライン時の新規アクションの作成(Create New Action If Uplink Goes Offline)*】ダイアログウィンドウが開きます。
2. **次の設定を行います。**
   名前(Name): アクションを説明する名前を入力します。

   タイプ(Type): アクションを定義する接続タイプを選択します。

   - **IPsecトンネル(IPsec Tunnel)**: IPsecトンネルに対するアクションを定義する場合は、ドロップダウンリストからこのオプションを選択します。
   - **追加アドレス(Additional Address)**: 追加アドレスに対するアクションを定義する場合は、ドロップダウンリストからこのオプションを選択します。

   IPsecトンネル(IPsec Tunnel):(【*IPsecトンネル(IPsec Tunnel)*】タイプにのみ利用可)IPsecトンネルを定義している場合は、ここでそれらのいずれかを選択できます。IPsecトンネルに関する詳細は、「*リモートアクセス*」>>「*IPsec*」の章を参照してください。

   追加。アドレス(Address):(【*追加アドレス(Additional Address)*】タイプのみ利用可)追加アドレスを定義している場合は、ここでそれらのいずれかを選択できます。追加アドレスに関する詳細は、「*インタフェースおよびルーティング*」>>「*インタフェース*」>>「*追加アドレス*」の章を参照してください。

   アクション(Action): ここで【*有効(Enable)*】または【*無効(Disable)*】のいずれかを選択できます。つまり、アップリンクが中断した場合は、上記で選択したIPsecトンネルや追加アドレスが有効または無効になるように設定します。

   コメント(Comment)(オプション):説明などの情報を追加します。
3. **【*保存(Save)*】をクリックします。**
   アクションは保存され、アップリンクの接続が中断すると適用されます。

アクションを編集または削除するには、対応するボタンをクリックします。

6.8.3詳細

【*アップリンクモニタリング(Uplink Monitoring)*】>>【*詳細(Advanced)*】タブで、アップリンク接続の自動モニタリングを無効にし、モニタリング(監視)に使用する1つ以上のホストを定義できます。これらのホストに対しては一定期間pingが行われ、それらのどれにも到達できない場合は、アップリンク接続はダウンしていると判断されます。その後、【*アクション(Action)*】タブで定義したアクションが実行されます。

モニタリングにお客様のホストを使用するには、以下の手順に従います。

1. **【*自動モニタリング(Automatic Monitoring)*】チェックボックスのチェックを外します。**
   【*モニタリングホスト(Monitoring Hosts)*】オブジェクトボックスが編集可能になります。
2. **【*モニタリングホスト(Monitoring Hosts)*】ボックスに1つ以上のホストを追加します。**
   オブジェクトリストからホストを選択するか、あるいは新しいホストを作成します。
3. **設定を保存するには【*適用(Apply)*】をクリックします。**

   設定が保存されます。これで、定義したホストがモニタリングに使用されます。

7 ネットワークサービス

この章では、ご利用のネットワーク用にAstaro Security Gatewayの複数のネットワークサービスを設定する方法を説明します。

この章には次のトピックが含まれます。

- DNS
- DHCP
- NTP

7.1 DNS

*【ネットワークサービス(Network Services)】>>【DNS】*メニューにあるタブには、さまざまな設定オプションがあり、すべて*ドメインネームシステム*(DNS)に関連しています。DNSとは、主にドメイン名(コンピュータのホスト名)をIPアドレスに変換するために使用されるシステムです。

7.1.1 グローバル

*【ネットワークサービス(Network Services)】>>【DNS】>>【グローバル(Global)】*タブでは、ゲートウェイを再帰的なDNSリゾルバとして使用することを許可するネットワークを指定できます。ここでは通常、内部ネットワークを選択します。

注 - 内部DNSサーバをActive Directoryの一部などとしてすでに起動している場合、このボックスは空のまま残します。

リゾルバキャッシュをクリア(Flush Resolver Cache)

DNSプロキシでは、レコードに対してキャッシュを使用します。各レコードには有効期限(TTL、生存時間)があり、この時間にレコードは削除されます。通常は1日に設定されています。ただし、キャッシュは手動で空にすることもできます(TTLが失効する前にDNSレコードの最新の変更を今すぐ有効にしたい場合など)。キャッシュを空にするには、*【今すぐリゾルバキャッシュをクリア(Flush Resolver Cache Now)】*をクリックします。

7.1.2フォワーダ

*【ネットワークサービス(Network Services)】>>【DNS】>>【フォワーダ(Forwarders)】*タブでは、いわゆるDNSフォワーダを指定できます。DNSフォワーダとは、ネットワーク上にあるDNS*(ドメインネームシステム)*サーバであり、外部DNS名に関するDNSクエリを当該ネットワーク外のDNSサーバに転送(フォワーディング)するために使用します。可能な限り、設定にDNSフォワーダを追加してください。DNSフォワーダは、お客様のサイトの「近く」にあり、(可能であれば)同じインターネットプロバイダが提供しているホストにする必要があります。これは「親」キャッシュとして使用されます。これにより、DNS要求の速度が飛躍的に向上します。転送を行うネームサーバを指定しないと、ゾーン情報についてのクエリ(問い合わせ)は最初にルートDNSサーバに対して行われるため、要求が完了するまで時間がかかります。

DNSフォワーダを選択するには、次の手順に従ってください。

1. **DNSフォワーダを選択します。**
   DNSフォワーダを選択または追加します。

   ISPが割り当てたフォワーダを使用(Use Forwarders Assigned By ISP)(オプション):DNSクエリをISPのDNSサーバに転送する場合は、*【ISPが割り当てたフォワーダを使用(Use Forwarders Assigned By ISP)】*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れると、ISPによって自動的に割り当てられたすべてのフォワーダがボックスの下に一覧表示されます。

2. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

7.1.3リクエストルーティング

内部DNSサーバが稼働しており、DNSフォワーダに解決させたくないドメインがある場合、そのドメインへのクエリをフォワーダではなく内部サーバに処理させることができます。*【ネットワークサービス(Network Services)】>>【DNS】>>【リクエストルーティング(Request Routing)】*タブで、独自のDNSサーバへのルートを定義することができます。

DNSリクエストルートを作成するには、次の手順に従います。

1. ***【リクエストルーティング(Request Routing)】*タブで*【新規DNSリクエストルート(New DNS Request Route)】*をクリックします。**
   *【新規DNSリクエストルートの作成(Create New DNS Request Route)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ドメイン(Domain): 代替DNSサーバを使用したいドメインを入力します。

   ターゲットサーバ(Target Servers): 上記ステップで入力したドメインを解決するために使用するDNSサーバを1つ以上選択します。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいルートが*【DNSリクエストルート(DNS Request Route)】*リストに表示され、ただちに有効になります。

DNSリクエストルートを編集または削除するには、対応するボタンをクリックします。

7.1.4スタティックエントリ

独自のDNSサーバをセットアップせず、ネットワーク内のいくつかのホストに対してスタティックDNSマッピングが必要な場合は、ここでこれらのマッピングを入力することができます。これは限られた数のエントリにしか対応できないため、フルオペレーションを行っているDNSサーバの代わりに使用することは決してしないでください。

スタティックマッピングを作成するには、次の手順に従います。

1. ***【スタティックエントリ(Static Entries)】*タブで、*【新規スタティックDNSマッピング(New Static DNS Mapping)】*をクリックします。**
   *【新規スタティックDNSマッピングの作成(Create New Static DNS Mapping)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ホスト名(Hostname): スタティックDNSマッピングを定義したいホストの完全修飾ドメイン名(FQDN)を入力します。

   IPv4アドレス(IPv4 Address): ホストのIPv4アドレスを入力します。

   IPv6アドレス(IPv6 Address): ホストのIPv6アドレスを入力します。

   リバースDNS(Reverse DNS): ホストのIPアドレスと名前のマッピングを有効化するには、チェックボックスにチェックを入れます。同じIPアドレスに複数の名前をマッピングすることが可能ですが、1つのIPアドレスには1つの名前にしかマッピングできません。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいマッピングが*【スタティックエントリ(Static Entries)】*リストに表示されます。

スタティックエントリを編集または削除するには、対応するボタンをクリックします。

7.1.5DynDNS

ダイナミックDNS(略してDynDNS)は、可変IPアドレスを持つコンピュータに静的インターネットドメイン名を割り当てることを可能にするドメインネームサービスです。DynDNS Webサイトで DynDNSサービスにサインアップし、DNSエイリアスを取得すると、アップリンクIPアドレスの変化に応じてこのエイリアスが自動的に更新されます。このサービスに登録すると、設定に必要なホスト名、ユーザ名、パスワードが提供されます。

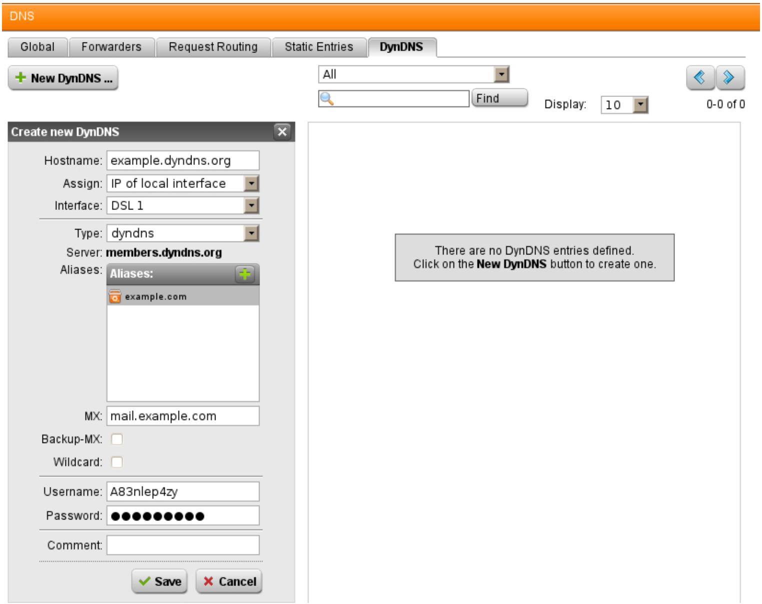


図63 DNS:DynDNSの設定

DynDNSを設定するには、次の手順に従ってください。

1. **[DynDNS]タブで、[新規DynDNS(New DynDNS)]をクリックします。**
   *[新規DynDNSの作成(Create New DynDNS)]*ダイアログボックスが開きます。

2. **次の設定を行います。**
   ホスト名(Hostname): DynDNSサービスプロバイダから受け取ったドメインを入力します(`example.dyndns.org`など)。ここでは、特定の構文を遵守してホスト名を入力する必要はありません。ここで入力が必要な内容は、各DynDNSサービスプロバイダの要件に

応じて異なります。DynDNSホスト名をゲートウェイのメインホスト名として使用することもできますが、必須ではありません。

割り当て(Assign): DynDNS名を関連付けるIPを定義します。ローカルインタフェースがパブリックIPアドレスを持つ場合は、このローカルインタフェースのIPを選択すると便利です。通常は、DSLアップリンクに対してこのオプションを使用します。【*デフォルトルートの最初のパブリックIP(First Public IP on the Default Route)*】を選択する場合、インタフェースの指定は不要です。代わりに、ASGがパブリックDynDNSサーバにWWW要求を送信し、パブリックDynDNSサーバは現在使用中のパブリックIPを返します。これは、プライベートネットワーク内部にあるASGがパブリックIPアドレスを持っておらず、マスカレーディングルータ経由でインターネットに接続している場合に有用です。

インタフェース(Interface): DynDNSサービスを使用するインタフェースを選択します。最も可能性が高いのは、インターネットに接続された外部インタフェースです。

タイプ(Type): 次のDynDNSタイプを使用できます。

- **DynDNS**: このオプションは、DynDNSの標準DNSサービスを使用している場合に選択します。
- **DynDNS-カスタム(DynDNS-custom)**: このオプションは、DynDNSのカスタムDNSサービスを使用している場合に選択します。カスタムDNSは、主にユーザ自身が所有または登録しているドメインを使用するために設計されています。

エイリアス(Aliases)(オプション):このダイアログボックスは、前述のメインホスト名と同じIPアドレスをポイントする追加ホスト名を入力するために使用します(`mail.example.com`、`example.com`など)。

MX(オプション):MX(mail exchanger)は、ホスト名で指定されたサーバ以外にメールを送信するために使用します(【*DynDNSタイプ(DynDNS Type)*】で【*DynDNS*】を選択した場合のみ使用可能)。MXレコードは、特定ドメインへのメールの送信先となるホスト(サーバ)を指定するという目的のために使用します。たとえば、MXとして`mail.example.com`を指定すると、`user@example.com`宛てのメールはホストである`mail.example.com`に配信されます。

バックアップ-MX(Backup-MX)(オプション):【*ホスト名(Hostname)*】テキストボックスで指定したホスト名がメインMXとなる場合のみ、このチェックボックスにチェックを入れます。すると、【*MX*】テキストボックスのホスト名はバックアップMXとしてのみアドバタイズされます。

ワイルドカード(Wildcard)(オプション):このオプションは、登録したドメインと同じIPアドレスをサブドメインのポイント先とする場合に選択します(【*DynDNSタイプ(DynDNS Type)*】で【*DynDNS*】を選択した場合のみ使用可能)。このオプションを使用すると、ドメ

インにワイルドカードとしてアスタリスク(*)が追加されます(`*.example.dyndns.org`など)。これにより、`www.example.dyndns.org`などが`example.dyndns.org`と同じアドレスをポイントするようになります。

ユーザ名(Username): DynDNSサービスプロバイダから受け取ったユーザ名を入力します。

パスワード(Password): DynDNSサービスプロバイダから受け取ったパスワードを入力します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいDynDNSが*DynDNS*リストに表示されます。サービスは無効になっています(ステータスアイコンは赤)。

4. **DynDNSを有効にします。**
   DynDNSサービスを有効にするには、ステータスアイコンをクリックします。

   サービスが有効になります(ステータスアイコンは緑)。

DynDNSを編集または削除するには、対応するボタンをクリックします。

複数のDynDNSオブジェクトを同時に使用することができます。2つのホスト名のすべての設定が同じであれば、別オブジェクトを2つ作成するのではなく、*【エイリアス(Aliases)】*オプションを使用することを推奨します。

7.2DHCP

DHCP*(Dynamic Host Configuration Protocol)*は、定義されたIPアドレスプールからクライアントコンピュータにアドレスを自動的に割り当てます。大規模ネットワークにおけるネットワーク設定を簡素化し、アドレスの衝突を防止するために設計されています。DHCPはクライアントに、IPアドレス、デフォルトのゲートウェイ情報、DNS設定情報を割り当てます。

クライアントコンピュータの設定を簡素化し、モバイルコンピュータが複数のネットワークを問題なく行き来できるようにすることに加え、DHCPはIPアドレスに関連する問題の原因特定とトラブルシューティングもサポートします。これは、DHCPサーバ自体の設定に問題があることが多いためです。また、アドレスを必要に応じて割り当てて、不要な場合は再利用することができるため、すべてのコンピュータが同時にアクティブになっていない場合などに、アドレススペースの使用をより効率化することができます。

7.2.1 サーバ

*【ネットワークサービス(Network Services)】>>【DHCP】>>【サーバ(Server)】*タブでは、DHCPサーバを設定することができます。Astaro Security Gateway は、接続されたネットワークに対してDHCPサービスを提供します。DHPCサーバを使用して、クライアントに基本ネットワークパラメータを割り当てることができます。それぞれ独自の構成が設定されている複数のインタフェース上でDHCPサービスを実行できます。

DHCPサーバを設定するには、次の手順に従ってください。

1. ***【サーバ(Servers)】*タブで、*【新規DHCPサーバ(New DHCP Server)】*をクリックします。**
   *【新規DHCPサーバを作成(Create New DHCP Server)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   インタフェース(Interface): IPアドレスをクライアントに割り当てるインタフェース。すでに設定されているインタフェースのみを選択できます。

   レンジの先頭/末尾(Range Start/End): そのインタフェースのアドレスプールとして使用するIPレンジ。デフォルトで、ネットワークカードに設定されたアドレスエリアがテキストボックスに表示されます。範囲は、インタフェースに接続されたネットワーク内である必要があります。

   DNSサーバ1/2(DNS Server 1/2): DNSサーバのIPアドレス。

   デフォルトゲートウェイ(Default Gateway): デフォルトゲートウェイのIPアドレス。

   > **注 -** ワイヤレスアクセスポイントとREDアプライアンスの両方で、デフォルトゲートウェイが接続先インタフェースと同じサブネット内にある必要があります。

   ドメイン(Domain)(オプション):クライアントに送信されるドメイン名を入力します(例:`intranet.example.com`)。

   リース時間(Lease Time): DHCPサーバによって割り当てられた各IPアドレスは、特定の時間が経過すると期限切れになります。ここでは、その時間を秒数で定義できます。デフォルトは86400秒(1日)です。最低値は600秒(10分)で、最大値は2592000秒(1か月)です。

   スタティックマッピングのあるクライアントのみ(Clients with Static Mappings Only)(オプション):*【スタティックMAC/IPマッピング(Static MAC/IP Mappings)】*タブに

エントリがあるクライアントのみにDHCPサーバがIPアドレスを割り当てるようにするには、このオプションを選択します。

WINSノードタイプ(WINS Node Type):WINS*(Windows Internet Naming Service)*とは、マイクロソフトがWindowsに実装したNBNS*(NetBIOS Name Server)*であり、NetBIOSコンピュータ名用のネームサーバおよびサービスです。WINSサーバは、コンピュータ名をIPアドレスと一致させるデータベースとして機能するため、NetBIOSを使用しているコンピュータがTCP/IPネットワークのメリットを利用できるようになります。次のWINSノードタイプを使用できます。

- **設定しない(Do not set)**: WINSノードタイプは設定するのではなくクライアントに選択されます。
- **Bノード(WINSなし)(B-node(no WINS))**: Bノードシステムはブロードキャストのみを使用します。
- **Pノード(WINSのみ)(P-node(WINS only))**: PノードシステムはWINS(Windows name server)へのポイントツーポイントの名前問い合わせのみを使用します。
- **Mノード(ブロードキャスト後WINS)(M-node(Broadcast, then WINS))**: Mノードシステムは、まずブロードキャストしてから、ネームサーバに問い合わせを行ないます。
- **Hノード(WINS後ブロードキャスト)(H-node(WINS, then Broadcast))**: Hノードシステムは、まずネームサーバに問い合わせてから、ブロードキャストします。

WINSサーバ(WINS Server): 選択したWINSノードタイプに応じて、このテキストボックスが表示されます。WINSサーバのIPアドレスを入力します。

HTTPプロキシ自動設定の有効化(Enable HTTP Proxy Auto Configuration): ブラウザの自動プロキシ設定用にPACファイルを提供するには、このオプションを選択します。詳しくは、「*Webセキュリティ*」>>「*Webフィルタリング*」>>「*詳細*」の章で、「*プロキシの自動設定*」セクションを参照してください。

> **注 -** Microsoft Windowsでは現在、IPv6でHTTPプロキシの自動設定をサポートしていません。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
新しいDHCPサーバ定義がDHCPサーバのリストに表示され、ただちにアクティブになっています。

DHCPサーバ定義を編集または削除するには、対応するボタンをクリックします。

7.2.2リレー

*【ネットワークサービス(Network Services)】>>【DHCP】>>【リレー(Relay)】*タブでは、DHCPリレーを設定することができます。DHCPサービスは別のDHCPサーバによって提供され、ASGはリレーとして機能します。DHCPリレーを使用すると、ネットワークセグメントをまたいでDHCP要求および応答を転送することができます。DHCPサーバと、DHCPトラフィックが転送されるインタフェースのリストを指定する必要があります。

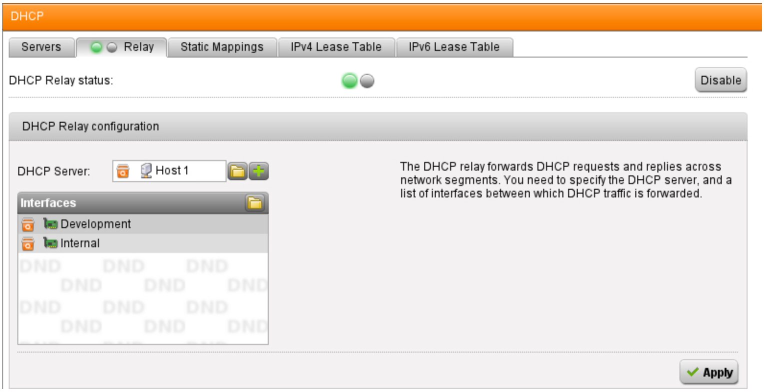


図64 DHCP: DHCPリレーの設定

DHCPリレーを設定するには、次の手順に従ってください。

1. ***【リレー(Relay)】タブで、【DHCPリレー(DHCP Relay)】を有効にします。***
ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【DHCPリレーの設定(DHCP Relay Configuration)】*エリアが編集可能になります。

2. **DHCPサーバを選択します。**

3. **インタフェースを選択します。**
これらのインタフェースに到着したDHCP要求は、選択されているDHCPサーバに転送されます。

4. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

設定をキャンセルするには、【*有効化を中止(Abort Enable)*】またはアンバー色のステータスアイコンをクリックします。

7.2.3スタティックMAC/IPマッピング

【*ネットワークサービス(Network Services)*】>>【*DHCP*】>>【*スタティックMAC/IPマッピング(Static MAC/IP Mappings)*】タブでは、一部または全部のクライアントに対するIPアドレスマッピングにスタティック(静的)MACアドレスを割り当てることができます。この目的のためには、設定されたDHCPサーバと、クライアントのネットワークカードのMACアドレスが必要です。MACアドレスは通常、2桁の16進数をコロンで区切って6組まとめた形式で指定します(`00:04:76:16:EA:62`など)。

注 - DHCPプールから通常通りに割り当てられたアドレスとスタティックにマッピングされたアドレスの間でIPアドレスの重複が発生することを防止するために、スタティックにマッピングする場合はDHCPプールの範囲外のアドレスを指定してください。たとえば、DHCPプールが`192.168.0.100`～`192.168.0.210`である場合にスタティックマッピングとして`192.168.0.200`を指定すると、2つのシステムが同じIPアドレスを持つことになります。

スタティックMAC/IPアドレスマッピングを作成するには、次の手順に従います。

1. ***【スタティックマッピング(Static Mappings)】*タブで、*【新規DHCPマッピング(New DHCP Mapping)】*をクリックします。**
   【*新規マッピング作成(Create New Mapping)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   DHCPサーバ(DHCP Server): スタティックMAC/IPマッピングに使用するDHCPサーバ。

   MACアドレス(MAC Address): クライアントのネットワークインタフェースカードのMACアドレス。

   IPアドレス(IP Address): クライアントのIPアドレス。IPアドレスは、ネットワークインタフェースカードのアドレス範囲内でなければなりません。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいマッピングが【*スタティックマッピング(Static Mappings)*】リストに表示されます。

スタティックMAC/IPマッピングを編集または削除するには、対応するボタンをクリックします。

7.2.4IPv4リーステーブル

DHCPを使用すると、クライアントはIPアドレスを持つのではなく、DHCPサーバからIPアドレスを*借りる(リースする)*ことになります。これにより、アドレスを一定期間にわたって使用する許可をクライアントに与えます。

DHCP

Servers | Relay | Static Mappings | **IPv4 Lease Table** | IPv6 Lease Table

Hostname	MAC address	IPv4 address	Lease start	Lease expiry	Add static mapping
[unknown]	[unknown]	10.8.1.1	2010/06/21 12:21:14 UTC	2010/06/21 12:21:14 UTC	New mapping
L041	00:1c:25:72:0f:83	10.8.1.2	2010/06/21 12:21:33 UTC	2010/06/22 12:21:33 UTC	New mapping
cs6	[unknown]	10.8.1.3	2010/06/21 12:21:51 UTC	2010/06/21 12:21:51 UTC	New mapping

図65 DHCP: IPv4リーステーブル

*【ネットワークサービス(Network Services)】>>【DHCP】>>【IPv4リーステーブル(IPv4 Lease Table)】*タブにある【リーステーブル(Lease Table)】には、DHCPサーバが現在発行しているリースが、開始日付やリースの有効期限日などの情報とともに表示されます。

スタティックマッピングの追加(Add Static Mapping)

テーブルの*【スタティックマッピングの追加(Add Static Mapping)】*列にある*【新規マッピング(New Mapping)】*ボタンを使用することにより、既存のリースを新しいスタティックMAC/IPマッピングのテンプレートとして使用することができます。以下の手順に従ってください。

1. ***【新規マッピング(New Mapping)】*ボタンをクリックします。**
   *【マッピングの追加(Add Mapping)】*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   MACアドレス(MAC Address)(オプション):MACアドレスは、スタティックマッピングを異なるホストに割り当てたい場合のみ変更してください。

   IPv4アドレス(IPv4 Address): DHCPプール範囲外のアドレスにIPアドレスを変更します。

   コメント(Comment)(オプション):説明などの情報を追加します。

   DNSマッピングの作成(Create DNS Mapping)(オプション):ホストへのスタティックDNSマッピングを自動的に作成する場合、このチェックボックスにチェックを入れます(*「ネットワークサービス」>>「DNS」>>「スタティックエントリ」*を参照)。*【ホスト名(Hostname)】*を指定すると、このマッピングで使用されます。

ネットワークホストオブジェクトの作成(Create Network Host Object)(オプション):ホストオブジェクトを自動的に作成する場合、このチェックボックスにチェックを入れます(*「定義およびユーザ」>>「ネットワーク定義」*を参照)。*【ホスト名(Hostname)】*を指定すると、これがオブジェクト名になります。

ホスト名(Hostname)(オプション):利便性のため、ホストの名前を指定しておくことをお勧めします。指定しないと、オブジェクトはリストに"[不明(unknown)]"と表示されます。

3. ***【保存(Save)】*をクリックします。**
設定が保存されます。

注 - リースをスタティックマッピングに変換する場合、DHCPプールの範囲外のIPアドレスに変更する必要があります。ただし、IPアドレスを変更しても、クライアントの使用するアドレスはすぐには変更されず、次にリース更新を試行するまで変更されません。

7.2.5IPv6リーステーブル

DHCPを使用すると、クライアントはIPアドレスを持つのではなく、DHCPサーバからIPアドレスを*借りる(リースする)*ことになります。これにより、アドレスを一定期間にわたって使用する許可をクライアントに与えます。

図66 DHCP:IPv6リーステーブル

*【ネットワークサービス(Network Services)】>>【DHCP】>>【IPv6リーステーブル(IPv6 Lease Table)】*タブにある【リーステーブル(Lease Table)】には、DHCPサーバが現在発行しているリースが、開始日付やリースの有効期限日などの情報とともに表示されます。

注 - プレフィックスアドバタイズメント経由で付与されたリースはテーブルに表示されません。

スタティックマッピングの追加(Add Static Mapping)

テーブルの*【スタティックマッピングの追加(Add Static Mapping)】*列にある*【新規マッピング(New Mapping)】*ボタンを使用することにより、既存のリースを新しいスタティックMAC/IPマッピングのテンプレートとして使用することができます。以下の手順に従ってください。

1. **【新規マッピング(New Mapping)】ボタンをクリックします。**
   *【マッピングの追加(Add Mapping)】*ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   DUIDアドレス(DUID Address)(オプション):DUIDアドレスは、スタティックマッピングを異なるホストに割り当てたい場合のみ変更してください。

   IPv6アドレス(IPv6 Address): DHCPプール範囲外のアドレスにIPアドレスを変更します。

   コメント(Comment)(オプション):説明などの情報を追加します。

   DNSマッピングの作成(Create DNS Mapping)(オプション):ホストへのスタティックDNSマッピングを自動的に作成する場合、このチェックボックスにチェックを入れます(*「ネットワークサービス」*>>*「DNS」*>>*「スタティックエントリ」*を参照)。*【ホスト名(Hostname)】*を指定すると、このマッピングで使用されます。

   ホスト用ネットワーク定義の作成(Create Network Definition For Host)(オプション):ホストオブジェクト用のネットワーク定義を自動的に作成する場合、このチェックボックスにチェックを入れます(*「定義およびユーザ」*>>*「ネットワーク定義」*を参照)。*【ホスト名(Hostname)】*を指定すると、これがオブジェクト名になります。

   ホスト名(Hostname)(オプション):利便性のため、ホストの名前を指定しておくことをお勧めします。指定しないと、オブジェクトはリストに"[不明(unknown)]"と表示されます。

3. **【保存(Save)】をクリックします。**
   設定が保存されます。

注 - リースをスタティックマッピングに変換する場合、DHCPプールの範囲外のIPアドレスに変更する必要があります。ただし、IPアドレスを変更しても、クライアントの使用するアドレスはすぐには変更されず、次にリース更新を試行するまで変更されません。

7.3NTP

【ネットワークサービス(Network Services)】>>*【NTP】*メニューを使用すると、接続されたネットワーク用のNTPサーバを設定することができます。NTP*(Network Time Protocol)*とは、IPネットワーク経由でコンピュータシステムのクロックの同期をとるために使用するプロトコルです。Astaro Security Gatewayの時刻の同期(*【マネジメント(Management)】*>>*【システム設定(System Settings)】*>>*【日付と時刻(Time and Date)】*タブで設定)だけではなく、特定のネットワークがこのサービスを使用できるように明示的に許可することもできます。

特定のネットワークに対してNTPによる時刻同期を有効にするには、次の手順に従ってください。

1. **NTPサーバを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。
2. **【*許可ネットワーク(Allowed Networks)*】を選択します。**
   NTPサーバへのアクセスを許可するネットワークを選択します。
3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

8 ネットワークセキュリティ

この章では、Astaro Security Gatewayの基本的なネットワークセキュリティ機能の設定方法について説明します。WebAdminの【*ネットワークセキュリティ統計(Network Security Statistics)*】ページには、送信元ホストと宛先ホストの両方に対する侵入防御イベントおよびドロップされたデータパケットの概要が表示されます。各セクションには、【*詳細(Detail)*】リンクが含まれています。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

この章には次のトピックが含まれます。

- ファイアウォール
- ネットワークアドレス変換(NAT)
- 侵入防御
- サーバロードバランシング
- ボイスオーバーIP(VoIP)
- 詳細設定

8.1 ファイアウォール

【*ネットワークセキュリティ(Network Security)*】>>【*ファイアウォール(Firewall)*】メニューを使用すると、ゲートウェイのファイアウォールルールを定義し、管理することができます。一般的に、ファイアウォールはゲートウェイの中核部分で、ネットワーク環境においてセキュリティポリシで禁止されている通信を妨げます。デフォルトのセキュリティポリシではAstaro Security Gateway ゲートウェイの他のソフトウェアコンポーネントが機能するために必要な、自動的に生成されたルールセットを除くすべてのネットワークトラフィックをブロックしてログします。ただし、自動的に生成されたルールセットは【*ファイアウォール(Firewall)*】>>【*ルール(Rules)*】タブには表示されません。このポリシでは、どのデータトラフィックにゲートウェイの通過を許可するかを明確に定義する必要があります。

8.1.1 ルール

【*ネットワークセキュリティ(Network Security)*】>>【*ファイアウォール(Firewall)*】>>【*ルール(Rules)*】では、ファイアウォールルールセットを管理できます。新規に定義したすべてのファイアウォールルールは、ルールテーブルに追加されると、デフォルトで無効になります。有効化されたファイアウォールルールは、最初のルールが一致するまで、所定の順序で適用されます。処理順

序は位置番号によって決まるため、位置番号によってルールの順序を変更すると、処理順序も変わります。

警告 - ファイアウォールルールが一致すると、他のすべてのルールは無視されます。そのため、ルールの順番は非常に重要です。*【すべて(送信元)(Any (Source))】–【すべて(サービス)(Any (Service))】–【すべて(宛先)(Any (Destination))】–【許可(アクション)(Allow (Action))】*のようなルールは、ルールテーブルの上部には配置しないでください。このようなルールをルールテーブルの上部に配置すると、各パケットがゲートウェイを双方向に通過できるようになり、以降の他のルールはすべて無視されます。

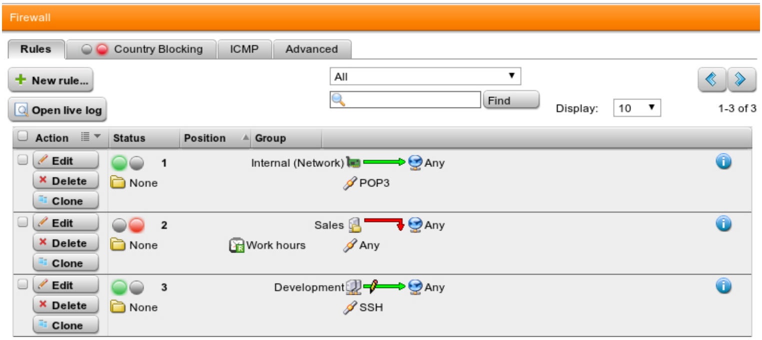


図67 ファイアウォール(Firewall):ルールテーブル

ファイアウォールルールを作成するには、次の手順に従います。

1. ***【ルール(Rules)】タブで、【新規ルール(New Rule)】をクリックします。***
   *【新規ルール作成(Create New Rule)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   グループ(Group):*【グループ(Group)】*オプションを使用すると、ファイアウォールルールを論理的にグループ化し、ファイアウォールルールセットを見やすくできます。グループ化は表示用のみで、ルールの一致には関係ありません。

   位置(Position): 位置番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

   送信元(Source): 送信元ネットワークの定義。パケットの送信元のホストまたはネットワークを説明します。

サービス(Service): プロトコルを説明するサービス定義。TCP、またはUDPの場合は、パケットの送信元および宛先ポートになります。

宛先(Destination): 宛先ネットワークの定義。パケットのターゲットホストまたはネットワークを説明します。

アクション(Action): アクションは、ルールに一致したトラフィックに対する処理を説明します。次のアクションを選択できます。

- **許可(Allow)**: 接続を許可し、トラフィックを送ります。
- **否認(Deny)**: このアクションが指定されたルールと一致したパケットは、警告なしでドロップされます。
- **リジェクト(Reject)**: このアクションが指定されたルールと一致した接続要求はアクティブに拒否されます。送信者にはICMPメッセージで通知されます。

期間(Time Period): デフォルトでは、期間定義は選択されていません。つまり、ルールは常に有効です。期間定義を選択すると、期間定義で指定された期間だけルールが有効になります。詳細は、「期間定義」を参照してください。

トラフィックのログ(Log Traffic): このオプションを選択すると、ログが有効になり、ルールに一致したパケットがファイアウォールログにログされます。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいルールが*【ルール(Rules)】*リストに表示されます。
4. **ルールを有効にします。**
   ルールを有効にするには、ステータスアイコンをクリックします。

ルールを編集または削除するには、対応するボタンをクリックします。

ライブログを開く(Open Live Log): フィルタされたパケットのリアルタイムログを含むポップアップウィンドウを開きます。表示は定期的に更新されて、最新のネットワークアクティビティが示されます。適用されたアクションによって、背景色が次のように変化します。

- 赤色:パッケージはドロップされました。
- 黄色:パッケージは拒否されました。
- 緑色:パッケージは許可されました。
- 灰色:アクションを決定できませんでした。

ライブログには、パケットが拒否される原因となったファイアウォールルールに関する情報も含まれます。こうした情報はルールのデバッグに不可欠です。

検索機能を使用して、特定エントリについてファイアウォールログをフィルタできます。検索機能では、表現の前にダッシュ(-)を付けることで、その表現を無効にできます。たとえば、`-WebAdmin`と指定すると、この表現を含むすべての行を連続して非表示にできます。

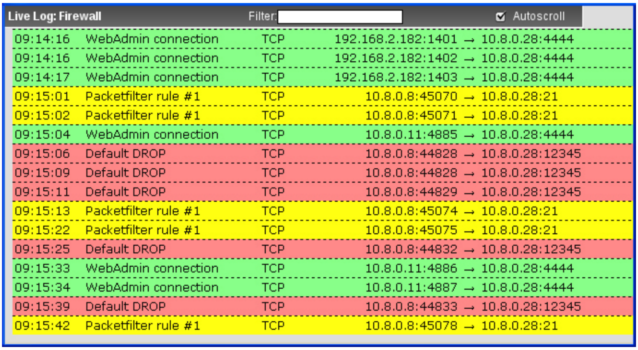


図68 ファイアウォール(Firewall):ライブログ

*【自動スクロール(Autoscroll)】*チェックボックスにチェックを入れると、ウィンドウのスクロールバーが自動的にスクロールダウンして、常に最新の結果が表示されます。

以下に、ファイアウォールの設定に関する基本的なヒントをいくつか示します。

- **ドロップされたブロードキャスト**: デフォルトでは、すべてのブロードキャストはドロップされ、ログもされません(詳細は「詳細」を参照)。この機能はNetBIOS(たとえば、Microsoft Windowsオペレーティングシステム)を使用する多数のコンピュータから成るネットワークで役立ちます。この理由は、ファイアウォールのログファイルは、ブロードキャストによってすぐにいっぱいになるからです。ブロードキャストのドロップルールを手動で定義するには、接続されたすべてのネットワークのブロードキャストアドレスの定義をグループ化し、`255.255.255.255/255.255.255.255`の"global_broadcast"定義を追加し、次にファイアウォール設定上部でこれらのアドレスに対するすべてのトラフィックをドロップするルールを追加します。ブロードキャストを多用するネットワークでは、これによってシステムのパフォーマンスも向上します。

- **IDENTトラフィックのリジェクト**:IDENT リバースプロキシを使用しない場合は、内部ネットワークのポート`113`(IDENT)へのトラフィックをアクティブに拒否できます。これにより、FTP、IRC、およびSMTPなどのIDENTを使用するサービスの長いタイムアウトを防止できます。

> **注 -** マスカレーディングを使用している場合は、マスカレードされているネットワークに対するIDENT要求が、マスカレードするインタフェースに届きます。

- NATはネットワークパケットのアドレスを変更するため、ファイアウォールの機能に影響を与えます。
  - DNATはファイアウォールの*前に*適用します。これは、ファイアウォールが、すでに変換されたパケットを「見る」ことを意味します。DNAT関連のサービスにルールを追加する際は、これを考慮することが必要です。
  - SNATおよびマスカレーディングはファイアウォールの*後に*適用されます。これは、ファイアウォールは、オリジナルの送信元アドレスを持つ変換されていないパケットをまだ「見る」ことを意味します。

テーブルヘッダのコントロールパネルを使用して、特定の基準でファイアウォールルールをフィルタして、読みやすいようにルールを再構成できます。グループを定義している場合は、ドロップダウンメニューからグループを選択し、このグループに属するすべてのルールを見ることができます。検索フィールドを使用して、キーワードあるいは単に文字列を探して、それに関連するルールを表示できます。検索は、ルールの送信元、宛先、サービス、グループ名、およびコメントで構成されます。

8.1.2送受信国別ブロック

*【ネットワークセキュリティ(Network Security)】>>【送受信国別ブロック(Country Blocking)】*タブで、特定国からの、または特定国へのトラフィックをブロックできます。1つの国あるいは大陸全体をブロックできます。このブロックは、ホストのIPアドレスのGeoIP情報に基づいています。

注 - 送受信国別ブロックは現在、IPv6ではサポートされていません。

送受信国別ブロックを有効にするには、以下の手順に従います。

1. **送受信国別ブロックを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり【*国(Countries)*】セクションが編集可能になります。
2. **ブロックする場所を選択します。**
   受信または送信トラフィックを完全にブロックする場所(国、地域)を1つ以上選択します。国の前にあるチェックボックスで国を選択するか、あるいは大陸セクションのヘッダのチェックボックスを選択して大陸全体を選択します。
3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。これで、選択した場所との間の受信および送信トラフィックがブロックされます。

ヒント – ヘッダバー右上のウィンドウアイコンをクリックして、大陸セクションを縮小できます。再度ウィンドウアイコンをクリックすると、大陸セクションが拡大します。

8.1.3ICMP

*【ネットワークセキュリティ(Network Security)】>>【ファイアウォール(Firewall)】>>【ICMP】*タブで、*インターネット制御メッセージプロトコル*(ICMP)の設定を構成できます。ICMPを使用して、ホスト間で接続関連のステータス情報をやり取りします。ICMPはネットワーク接続のテストやネットワークの問題のトラブルシューティングに重要です。

このタブで任意のICMPトラフィックを許可すると、ファイアウォールのICMP設定が上書きされます。特定のホストやネットワークだけにICMPを許可する場合は、*【ファイアウォール(Firewall)】>>【ルール(Rule)】*タブを使用します。

グローバルICMP設定(Global ICMP Settings)

以下のグローバルICMPオプションを利用できます。

- **ゲートウェイでICMPを許可する(Allow ICMP on Gateway)**: このオプションで、どの種類のICMPパケットにもゲートウェイが対応できるようにします。
- **ゲートウェイを通してICMPを許可する(Allow ICMP through Gateway)**: このオプションを使用すると、すべてのICMPパケットをゲートウェイを通して転送可能になります。
- **ICMPリダイレクトをログする(Log ICMP Redirects)**: ICMPリダイレクトは、パケットの宛先へのより良いルートを探すために、1台のルータから別のルータに送信されます。ルータはルーティングテーブルを変更して、より適切と想定されるルートを経由して同じ宛先にパケットを送ります。このオプションを選択すると、すべてのICMPリダイレクトがファイアウォールログに書き込まれます。

ping設定(Ping Settings)

*ping*プログラムは、IPネットワークを横断して特定ホストに到達できるかどうかをテストするためのコンピュータネットワークツールです。pingは、ICMP*エコー要求*パケットをターゲットホストに送信し、ICMP*エコー応答*による返信をリスンすることで機能します。pingは、間隔のタイミングと応答率を使用して、ホスト間の往復時間とパケット紛失率を評価します。

以下のpingオプションを利用できます。

- **ゲートウェイのping可視化(Gateway Is Ping Visible)**: ゲートウェイはICMP*エコー要求*パケットに応答します。この機能はデフォルトで有効になっています。

- **ゲートウェイからping(Ping From Gateway)**: ゲートウェイでpingコマンドを使用できます。この機能はデフォルトで有効になっています。
- **ゲートウェイでpingを転送(Gateway Forwards Pings)**: ゲートウェイがICMP*エコー要求*と*エコー応答*パケットを転送します。

traceroute設定(Traceroute Settings)

traceroute(トレースルート)プログラムは、IPネットワーク上でパケットが使用するルートの決定に使用されるコンピュータネットワークツールです。tracerouteは、パケットの伝送に関与したルータのIPアドレスを一覧表示します。一定の時間内にパケットのルートを判断できない場合は、IPアドレスの代わりにアスタリスク(*)で報告します。一定の回数だけ失敗すると、確認作業は終了します。確認の中断には多くの理由が考えられますが、ほとんどの場合は、ネットワークパスのファイアウォールがtracerouteパケットをブロックすることが原因となります。

以下のtracerouteオプションを利用できます。

- **ゲートウェイのtraceroute可視化(Gateway Is Traceroute Visible)**: ゲートウェイはtracerouteパケットに応答します。
- **ゲートウェイでtracerouteを転送(Gateway Forwards Traceroute)**: ゲートウェイでtraceroute パケットを転送します。

注 - さらに、UNIX tracerouteアプリケーション用のUDP ポートも開きます。

8.1.4詳細

*【ネットワークセキュリティ(Network Security)】>>【ファイアウォール(Firewall)】>>【詳細(Advanced)】*タブには、ファイアウォールおよびNATルールの詳細設定が含まれています。

コネクショントラッキングヘルパ(Connection Tracking Helpers)

コネクショントラッキングヘルパを使用することにより、複数のネットワーク接続を使用するプロトコルでファイアウォールあるいはNATルールを使用できます。ファイアウォールが取り扱うすべての接続は、*conntrack*カーネルモジュール(*コネクショントラッキング*プロセスとも呼ばれます)で追跡します。たとえば、FTP およびIRC などのプロトコルにはいくつかのポートを開くことが必要で、それらの正常な機能をサポートする特別なコネクショントラッキングヘルパが必要になります。これらのヘルパは特別なカーネルモジュールで、追加の接続をそれらを最初の接続に関連付けることによって(通常はデータストリームから関連するアドレスを読み取ることで)特定します。

たとえば、FTPの接続が正常に機能するには、FTP conntrackヘルパを選択する必要があります。これはFTPプロトコルの特異性によるもので、それによってFTPコントロールコネクションと呼ばれ

る単一の接続を確立します。この接続でコマンドが発行されると、他のポートが開いてその特定コマンドに関連するデータの残りを実行します(例:ダウンロードあるいはアップロード)。問題は、それらは動的にネゴシエートされたため、ゲートウェイがこれらの特別なポートを知らない、ということです。したがって、ゲートウェイは、これらの特定のポートでサーバをクライアントに接続させなければならないか(アクティブなFTP接続)、またはインターネット上でクライアントをFTPサーバに接続させなければならないか(パッシブなFTP接続)を知ることができません。

これがFTP conntrackヘルパが役に立つ理由です。この特別なヘルパは特別なコネクショントラッキングモジュールに追加され、特別な情報の制御接続(通常はポート21)をスキャンします。ヘルパが正しい情報に出会うと、その情報をコントロールコネクションの関連情報として想定される接続のリストに追加します。これにより、ゲートウェイで最初のFTP接続と関連する全接続の両方を追跡することが可能になります。

コネクショントラッキングヘルパは以下のプロトコルで使用できます。

- FTP
- IRC(DCC用)
- PPTP
- TFTP

注 - ファイアウォールでPPTP VPNサービスを提供したい場合は、PPTPヘルパモジュールをロードする必要があります。ロードしないと、PPTPセッションは確立できません。この理由は、PPTPは、別個のIPプロトコルの*Generic Routing Encapsulation*(GRE)通信に切り換える前に、TCPポート1723接続を確立するからです。PPTPヘルパモジュールをロードしないと、すべてのGREパケットはゲートウェイにブロックされます。PPTPヘルパモジュールを使用しない場合は、代わりにファイアウォールルールを手動で追加し、受信および送信トラフィックでGREパケットを許可します。

プロトコル処理(Protocol Handling)

TCPウインドウスケーリングを有効にする(Enable TCP Window Scaling):TCPの受信ウインドウ(RWin)サイズは、接続時にバッファできる受信データ量(バイト単位)です。送信側ホストは、受信側ホストからの受信確認とウィンドウの更新を待つ間、その量のデータのみを送信できます。高帯域幅ネットワークをさらに効率的に使用するために、大きなTCPウインドウサイズを使用できます。ただし、TCPウインドウサイズのフィールドはデータの流れを制御し、2バイトあるいは65535バイトのウインドウサイズに制限されています。サイズフィールドは拡張できないため、スケーリングファクタを使用します。TCPウインドウのスケーリングはTCP/IPスタックのカーネルオプションで、最大ウインドウサイズを65535バイトから1ギガバイトに拡大するために使用できます。ルー

タ、負荷バランサ、ゲートウェイなどの多くのネットワークデバイスはウインドウのスケーリングをまだ完全にはサポートしていないため、スケーリングはデフォルトでは無効になっています。

厳密なTCPセッション処理を使用する(Use Strict TCP Session Handling): デフォルトでは、システムはネットワーク機能のリセットによりコネクショントラッキングテーブルで現在扱われていない既存のTCP接続を「ピックアップ」できます。これはSSH およびTelnetなどの対話型セッションが、ネットワークインタフェースが一時的に利用できない場合に停止しないことを意味します。このオプションを有効にすると、そのようなセッションを再度確立するには新しい3WAYハンドシェークが常に必要になります。一般的にはこのオプションはオフのままにしておくことをお勧めしています。

パケット長の有効性を確認(Validate Packet Length): 有効にすると、ファイアウォールは、ICMP、TCP、またはUDPプロトコルの使用時に、データパケットが最小長を満たしているかチェックします。データパケットが最小値より小さい場合、それらはブロックされ、その記録がファイアウォール ログに書き込まれます。

なりすまし保護(Spoof Protection): デフォルトでは、なりすまし保護は無効になっています。以下の設定から選択できます。

- **通常(Normal)**: ゲートウェイは、インタフェース自体と同じ送信元IPアドレスを持つパケット、またはそのインタフェースに別に割り当てられたネットワークの送信元IPを持つインタフェースに到着するパケットを、ドロップしてログします。
- **厳密(Strict)**: ゲートウェイは、宛先IPにインタフェースが指定され、割り当てられた以外のインタフェースに到着する(つまり、宛先として指定されていないインタフェースに到着する)すべてのパケットを、ドロップしてログします。たとえば、内部ネットワークのみからパケットを受け付けると想定される内部インタフェースのIPアドレスに外部ネットワークから送信されたパケットはドロップされます。

ログオプション(Logging Options)

FTPデータコネクションをログ(Log FTP Data Connections): ASG は、ファイルおよびディレクトリリスティングのFTPデータコネクションをログします。ログレコードには「FTP data(FTPデータ)」という文字列によってマークが付けられます。

ユニークなDNS要求をログする(Log Unique DNS Requests): ASG は、DNSサーバへのすべての要求およびそれらの結果をログします。ログレコードには「DNS request(FTP要求)」という文字列によってマークが付けられます。

ドロップされたブロードキャストをログする(Log Dropped Broadcasts): デフォルトで、ファイアウォールはすべてのブロードキャストをドロップし、ログも行いません。ただし、ブロードキャストをファイアウォール ログに記録する必要がある場合は、このオプションを選択します(監査など)。

8.2NAT

【ネットワークセキュリティ(Network Security)】>>*【NAT】*メニューを使用すると、ゲートウェイのNATルールを定義し、管理することができます。*ネットワークアドレス変換*(NAT)とは、ルータやゲートウェイを通過するIPパケットの送信元アドレスまたは宛先アドレス(あるいは両方)を書き換えるプロセスです。NATを使用するほとんどのシステムは、プライベートネットワーク上の複数のホストが1つのパブリックIPアドレスを使用してインターネットにアクセスできるようにするためにNATを使用しています。あるクライアントがIPパケットをルータに送信すると、NATは送信アドレスを別のパブリックIPアドレスに変換してからインターネットにパケットを転送します。応答パケットを受信すると、NATはパブリックアドレスを元のアドレスに変換し、クライアントにパケットを転送します。システムリソースに応じて、NATは自己裁量で大規模内部ネットワークに対応できます。

8.2.1 マスカレード

マスカレードとは、*送信元ネットワークアドレス変換*(SNAT)の特殊ケースであり、ネットワークインタフェース(通常は、インターネットに接続された外部インタフェース)上の1つの公式IPアドレスの背後に内部ネットワーク(通常はプライベートアドレススペースを持つLAN)をマスカレードすることができます。SNATの場合、複数の送信元アドレスを複数の宛先アドレスにマッピングすることができるため、より汎用的です。

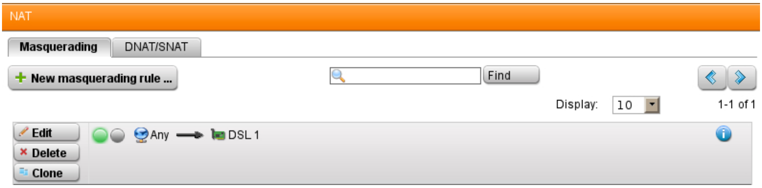


図69 NAT:マスカレードルールのリスト

注 - 送信元アドレスは、指定されたインタフェース経由でパケットがゲートウェイシステムから配信された場合にのみ変換されます。新しい送信元アドレスは常に、当該インタフェースの最新IPアドレスとなります(つまり、このアドレスは動的です)。

マスカレードルールを作成するには、次の手順に従います。

1. ***【マスカレード(Masquerading)】*タブで、*【新規マスカレードルール(New Masquerading Rule)】*をクリックします。**

【*新規マスカレードルールの作成(Create New Masquerading Rule)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   ネットワーク(Network): マスカレードする(内部)ネットワークを選択します。

   インタフェース(Interface): インターネットに接続する(外部)インタフェースを選択します。

   アドレスを使用(Use Address): 選択したインタフェースに複数のIPアドレスが割り当てられている場合(「*インタフェースおよびルーティング(Interfaces & Routing)*」>>「*追加アドレス*」参照)、マスカレードに使用するIPアドレスをここで定義できます。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
   新しいマスカレードルールがマスカレードルールのリストに表示されます。

4. **マスカレードルールを有効にします。**
   マスカレードルールを有効にするには、ステータスアイコンをクリックします。

ルールを編集または削除するには、対応するボタンをクリックします。

注 - クライアントが外部サーバにアクセスできるようにするには、ファイアウォールで内部ネットワークからインターネットへのトラフィックを許可する必要があります。

8.2.2DNAT/SNAT

DNAT*(Destination Network Address Translation)*とSNAT*(Source Network Address Translation)*は、いずれもNATの特殊ケースです。SNATでは、接続を開始したコンピュータのIPアドレスが書き換えられます。一方、DNATでは、データパケットの宛先アドレスが書き換えられます。DNATは、内部ネットワークでプライベートIPアドレスを使用しており、管理者が一部のサービスを外部からも使用可能にしたい場合に特に便利です。

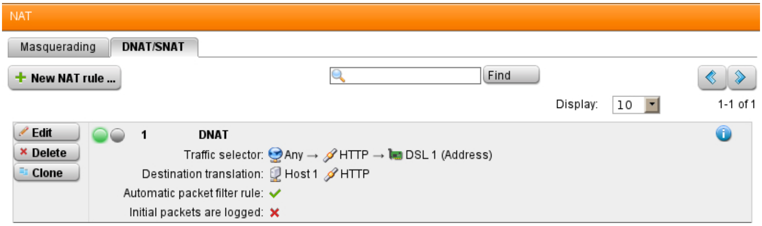


図70 NAT：DNAT/SNATルールのリスト

これは、例を使って説明するとわかりやすいでしょう。内部ネットワークでアドレススペース192.168.0.0/255.255.255.0を使用しており、WebサーバがIPアドレス192.168.0.20で機能しているとします。この場合、インターネットベースのクライアントでポート80を使用可能にする必要があります。192.168.アドレススペースはプライベートであるため、インターネットベースのクライアントはWebサーバにパケットを直接送信できません。ただし、ASGの外部(公開)アドレスと通信することはできます。この場合、DNATは、システムアドレスのポート80向けのパケットを捕捉し、内部Webサーバに転送できます。

注 - *PPTP VPNアクセス*はDNATに対応していません。

動的であるマスカレーディングとは異なり、SNATでは静的アドレス変換を使用します。つまり、それぞれの内部アドレスは、独自の外部から参照可能なIPアドレスに変換されます。

注 - デフォルトで、ポート443(HTTPS)はユーザポータルに使用されます。ポート443を内部サーバに転送する予定がある場合、*【マネジメント(Management)】>>【ユーザポータル(User Portal)】>>【詳細(Advanced)】*タブでユーザポータルのTCPポートを他の値(1443など)に変更する必要があります。

DNATはファイアウォールの前に行われるため、適切なファイアウォールルールを定義しておく必要があります。詳しくは、*「ネットワークセキュリティ」>>「ファイアウォール」>>「ルール」*を参照してください。

DNAT/SNATルールを定義するには、次の手順に従います。

1. ***【DNAT/SNAT】タブで、【新規NATルール(New NAT Rule)】をクリックします。***
   *【新規NATルールの作成(Create New NAT Rule)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name)：NATルールを説明する名前を入力してください。

グループ(Group): グループは、複数のNATルールを論理的に組み合わせて読みやすくするために便利です。グループは任意の文字列にできます。

位置(Position): 位置番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

トラフィック送信元(Traffic Source): パケットのオリジナルの送信元アドレス(1つのホストにすることも、ネットワーク全体にすることもできます)。

トラフィックサービス(Traffic Service): パケットのオリジナルのサービスタイプ(送信元ポートと宛先ポート、およびプロトコルタイプから構成されています)。

> **注 -** トラフィックサービスは、対応するアドレスも変換される場合のみ変換できます。さらに、2つのサービスが同じプロトコルが使用する場合のみ、サービスを別のサービスに変換できます。

トラフィック宛先(Traffic Destination): パケットのオリジナルの宛先アドレス(1つのホストにすることも、ネットワーク全体にすることもできます)。

NATモード(NAT Mode): ネットワークアドレス変換モードを選択します。選択に応じて、さまざまなオプションが表示されます。次のモードを使用できます。

- **NATなし(No NAT)**: このオプションは例外ルールの一種と考えることができます。たとえば、定義したネットワークにNATルールがある場合、このネットワーク内の特定のホストに対して【*NATなし(No NAT)*】ルールを作成することができます。これにより、これらのホストはNATの対象外となります。
- **DNAT(宛先)(DNAT(Destination))**: *DNAT*を選択する場合、宛先ホスト/ネットワークと宛先サービス(パケットの新しい宛先アドレスとサービス)を選択します。
- **SNAT(送信元)(SNAT(Source))**: *SNAT*を選択する場合、送信元ホスト/ネットワークと送信元サービス(パケットの新しい送信元アドレスとサービス)を選択します。
- **フルNAT(Full NAT)**: *フルNAT*を選択する場合、宛先ホスト/ネットワークと宛先サービス、そして送信元ホスト/ネットワークと送信元サービスを選択します。

初期パケットのログ(Log Initial Packets)(オプション): このオプションは、通信の初期化パケットをファイアウォールログに書き込む場合に選択します。これにより、NATルールを使用する場合はいつでも、ファイアウォールログに「NATを使用する接続(Connection

using NAT)」というメッセージが記述されます。このオプションは、ステートフルプロトコルでもステートレスプロトコルでも機能します。

自動 ファイアウォールルール(Automatic Firewall Rules)(オプション):このオプションは、ゲートウェイルールを自動生成する場合に選択します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   新しいルールが*【DNAT/SNAT】*リストに表示されます。

4. **NATルールを有効にします。**
   NATルールを有効にするには、ステータスアイコンをクリックします。

ルールを編集または削除するには、対応するボタンをクリックします。

8.3侵入防御

*【ネットワークセキュリティ(Network Security)】>>【侵入防御(Intrusion Prevention)】*メニューで、ゲートウェイのIPSルールを定義し、管理することができます。*侵入防御システム*(IPS)は、シグニチャに基づくIPSルールセットを利用して攻撃を認識します。システムは、トラフィックを完全に分析し、ネットワークに到達する前に攻撃を自動的にブロックします。既存のルールセットと攻撃パターンは、パターン更新によって最新状態に更新されます。新しいIPS攻撃パターンのシグニチャは、IPSルールとしてルールセットに自動的にインポートされます。

8.3.1グローバル

*【ネットワークセキュリティ(Network Security)】>>【侵入防御(Intrusion Prevention)】>>【グローバル(Global)】*タブでは、Astaro Security Gatewayの*侵入防止システム*(IPS)を有効化することができます。

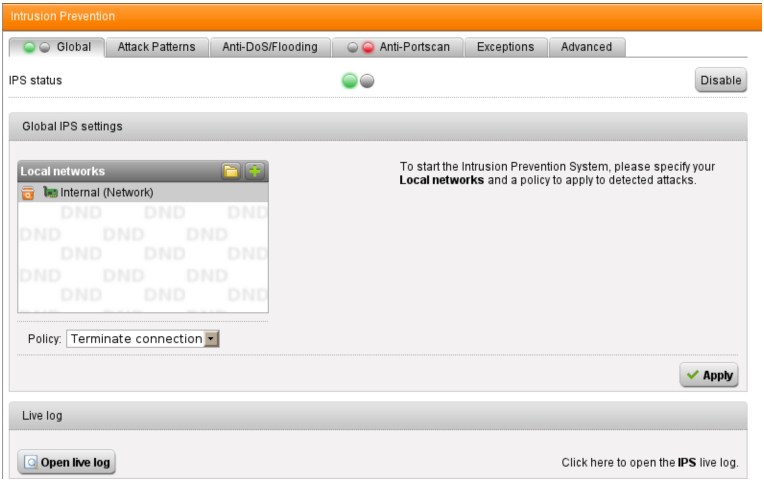


図71 IPS:侵入防御を有効にする

IPSを有効にするには、次の手順に従ってください。

1. **侵入防御システムを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色になり、【*グローバルIPS設定(Global IPS Settings)*】エリアが編集可能になります。

2. **次の設定を行います。**
   ローカルネットワーク(Local Networks): 侵入防御システムで防御するネットワークを選択します。ローカルネットワークを選択しないと、侵入防御は自動的に無効になり、トラフィックはモニタリングされません。

   ポリシ(Policy): ブロッキングルールがIPS攻撃シグネチャを検出したときに侵入防御システムが使用するセキュリティポリシを選択します。

   - **サイレントドロップ(Drop Silently)**: データパケットは、他のアクションなしでドロップされます。
   - **接続中止(Terminate Connection)**: 中止データパケット(TCPの場合は*RST*、UDP接続の場合は*ICMP Port Unreachable*)が両方の通信パートナーに送信され、接続が終了します。

> **注 -** デフォルトでは【*サイレントドロップ(Drop Silently)*】が選択されています。通常はこの設定を変更する必要はありません。これは特に、疑わしい侵入者に中止データパケットが悪用され、ゲートウェイについての情報が引き出されてしまう可能性があるためです。

3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

ライブログ

侵入防御ライブログは、選択したIPSルールのモニタリングに使用できます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

8.3.2攻撃パターン

【*ネットワークセキュリティ(Network Security)*】>>【*侵入防御(Intrusion Prevention)*】>>【*攻撃パターン(Attack Patterns)*】タブには、共通の攻撃パターンに従ってグループ分けされたIPSルールが表示されます。攻撃パターンは次のようにまとめられています。

- **オペレーティングシステム固有の攻撃(Operating System Specific Attacks)**: オペレーティングシステム関連の脆弱性を悪用しようとする攻撃。
- **サーバに対する攻撃(Attacks Against Servers)**: Webサーバ、メールサーバなどあらゆる種類のサーバを対象とする攻撃。
- **クライアントソフトウェアに対する攻撃(Attacks Against Client Software)**: Webブラウザ、マルチメディアプレーヤなどのクライアントソフトウェアを対象とする攻撃。
- **プロトコル異常(Protocol Anomaly)**: ネットワークの異常を探す攻撃パターン。
- **マルウェア(Malware)**: 所有者のインフォームドコンセントなく、コンピュータシステムへの侵入や破壊を行うように設計されたソフトウェア(トロイの木馬、DoS通信ツールなど)。

パフォーマンス向上のために、会社のローカルネットワークに導入されているサービスまたはソフトウェアに該当しないチェックボックスはチェックを外してください。たとえば、ローカルネットワーク内でWebサーバを運用していない場合は、【*HTTPサーバ(HTTP Servers)*】用の選択を取り消すことができます。

各グループに対して、次の設定を使用できます。
アクション(Action): デフォルトで、グループ内の各ルールにはアクションが関連付けられています。次のアクションを選択できます。

- **破棄(Drop)**: デフォルト設定。攻撃の疑いがある試行が見つかると、その原因であるデータパケットはドロップされます。
- **警告(Alert)**:【*破棄(Drop)*】設定と違い、重大なデータパケットはゲートウェイを通過できますが、IPSログにアラートメッセージが記述されます。

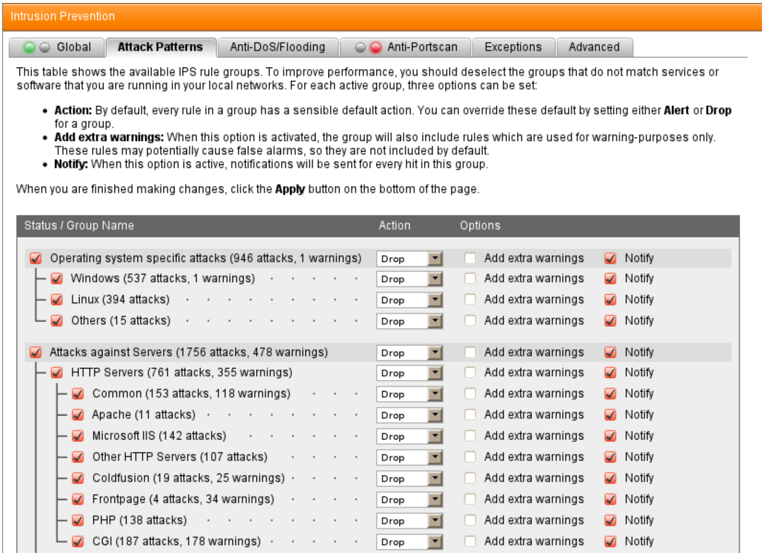


図72 IPS:攻撃パターン

> **注 -** 個々のIPSルールの設定を変更するには、【*侵入防御(Intrusion Prevention)*】>>【*詳細(Advanced)*】タブの【*変更されたルール(Modified Rules)*】ボックスを使用します。Astaro Security GatewayV8で使用されているIPSルールの詳細なリストは、Astaro のWebサイトで参照できます。

追加の警告ルールを有効にする(Add Extra Warnings): このオプションを選択すると、各グループにルールが追加され、IPS検出率が向上します。これらのルールは、明示的な攻撃パターンよりも一般的で曖昧なので、アラートの数が増える可能性があります。このため、これらのルールのデフォルトアクションは【*警告(Alert)*】であり、設定はできません。

通知(Notify): このオプションを選択すると、このグループと一致するIPSイベントが発生するたびに管理者に通知が送信されます。このオプションが有効になるのは、【*マネジメント(Management)*】>>【*通知(Notifications)*】>>【*通知(Notifications)*】タブで侵入防止システムの通知機能を有効にした場合のみです。さらに、送信される通知のタイプ(つまり、Eメー

ルまたはSNMPトラップ)は、ここでの設定によって決まります。また、通知設定の変更が有効になるまでは最大5分かかる場合があります。

8.3.3DoS/フラッド防御

*【DoS/フラッド防御(Anti-DoS/Flooding)】*タブでは、DoS(*サービス拒否*)攻撃とDDoS(*分散型サービス拒否*)攻撃から防御するためのオプションを設定できます。

一般にDoS攻撃とDDoS攻撃は、正当な要求がコンピュータリソースを使用できないようにします。シンプルな例では、攻撃者はサーバに無意味なパケットを送信して過負荷をかけ、パフォーマンスに負担をかけます。このような攻撃には大規模な帯域幅が必要となるため、いわゆる*SYNフラッド攻撃*を使用する攻撃者が増え続けています。この攻撃は、帯域幅の過負荷ではなく、システムリソースのブロックを目的としています。この目的のために、攻撃者は多くの場合、偽造された送信元アドレスを使用してサービスのTCPポートにSYNパケットを送信します。これに対し、サーバはTCP/SYN-ACKを送り返して、これに応答する送信元アドレスからのTCP/ACKパケットを待ち続けるため、接続がhalf-open状態になります。ところが、送信元アドレスは偽造されているため、応答は返ってきません。これらのhalf-open状態の接続により、サーバが対応できる接続数が飽和状態になり、正当な要求に対応できなくなります。

このような攻撃は、特定時間内にネットワークに対して送信されるSYN(TCP)、UDP、ICMPパケットの数を制限することで回避できます。

TCP SYNフラッド防御

SYN(TCP)フラッド防御を有効にするには、次の手順に従います。

1. ***【DoS/フラッド防御(Anti-DoS/Flooding)】*タブで、*【TCP SYNフラッド防御の使用(Use TCP SYN Flood Protection)】*チェックボックスにチェックを入れます。**
2. **次の設定を行います。**
   モード(Mode): 次のモードを使用できます。

   - **送信元アドレスと宛先アドレスの両方(Both Source and Destination Addresses)**: 送信元IPアドレスと宛先IPアドレスの両方と一致するSYNパケットをドロップする場合、このオプションを選択します。まず、送信元IPアドレスと一致するSYNパケットがフィルタされます。次に、要求がまだ多すぎる場合には、宛先IPアドレスに従って追加でフィルタされます。このモードはデフォルトで設定されています。
   - **宛先アドレスのみ(Destination Address Only)**: 宛先IPアドレスのみに従ってSYNパケットをドロップする場合、このオプションを選択します。

- **送信元アドレスのみ(Source Address Only)**: 送信元IPアドレスのみに従ってSYNパケットをドロップする場合、このオプションを選択します。

ログ(Logging): このオプションを使用すると、ログレベルを選択できます。以下のレベルを設定できます。

- **オフ(Off)**: ログを完全にオフにする場合は、このログレベルを選択します。
- **制限(Limited)**: ログを1秒あたり5パケットに制限する場合、このログレベルを選択します。デフォルトではこのレベルが設定されています。
- **すべて(Everything)**: すべてのSYN(TCP)接続試行を詳細にログする場合、このログレベルを選択します。SYN(TCP)フラッド攻撃により、ログが膨大になる可能性があります。

送信元パケットレート(Source Packet Rate): ここに、送信元IPアドレスに対して許可される1秒あたりのパケットレートを指定できます。

宛先パケットレート(Destination Packet Rate): ここに、宛先IPアドレスに対して許可される1秒あたりのパケットレートを指定できます。

> **注 -** ここで合理的な値を入力することは重要です。レートを高く設定し過ぎると、Webサーバがそのように大量なSYN(TCP)パケットに対処しきれず、障害が発生する可能性などがあります。一方、レートを低く設定し過ぎると、ゲートウェイが通常のSYN(TCP)要求をブロックして、予期しない挙動をする可能性があります。各システムの合理的な設定は、ハードウェアに大きく依存します。従って、システムに適した値にデフォルト値を置き換えてください。

3. ***【適用(Apply)】をクリックします。***
   設定が保存されます。

UDPフラッド防御

*UDPフラッド防御*機能は、UDPパケットフラッドを検出し、ブロックします。

*UDPフラッド防御*の設定は、*TCP SYNフラッド防御*の設定と同じです。

ICMPフラッド防御

*ICMPフラッド防御*機能は、ICMPパケットフラッドを検出し、ブロックします。

*ICMPフラッド防御*の設定は、*TCP SYNフラッド防御*の設定と同じです。

8.3.4ポートスキャン防御

*【ネットワークセキュリティ(Network Security)】>>【侵入防御(Intrusion Prevention)】>>【ポートスキャン防御(Anti-Portscan)】*タブでは、一般的なポートスキャン検出オプションを設定することができます。

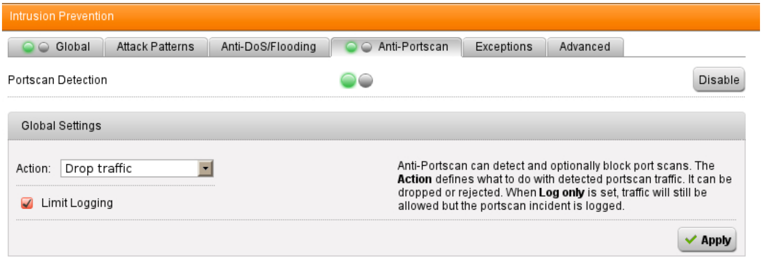


図73 IPS:ポートスキャン防御の設定

ポートスキャンとは、セキュアなシステムで使用可能なサービスを探るためにハッカーが用いる手段です。攻撃者は、システムに侵入したり、DoS攻撃を開始するために、ネットワークサービスに関する情報を必要としています。このような情報を入手すると、攻撃者はこれらのサービスにあるセキュリティ上の欠陥を悪用しようとします。インターネットプロトコルTCPおよびUDPを使用しているネットワークサービスは、特別なポートからアクセス可能であり、このポート割り当ては一般によく知られています。たとえば、SMTPサービスはTCPポート25に割り当てられています。サービスで使用されるポートは、オープンであると見なされます。これは、このようなポートへの接続を確立することができるためです。一方、使用されていないポートはクローズと見なされ、これらのポートへの接続を試みると失敗します。攻撃者は、ポートスキャナという特別なソフトウェアツールを利用してオープンポートを探します。このプログラムは、攻撃対象のコンピュータ上にある複数のポートに対して接続を試みます。接続が成功したポートはオープンであるとツールに表示されます。こうして攻撃者は、攻撃対象のコンピュータにおいてどのネットワークサービスが使用可能であるかを示す必要な情報を入手します。

インターネットプロトコルTCPとUDPでは、使用可能なポートが全部で65535個あるため、ポートは非常に短い間隔でスキャンされます。サービスへ接続しようとする試行が異常に大量に発生していることをゲートウェイが検出した場合(特に、これらの試行が同じ送信元アドレスから送信されている場合)、ゲートウェイがポートスキャンを受けている可能性が高くなります。攻撃者の疑いのある人がネットワーク上のホストまたはサービスのスキャンを行うと、ポートスキャン検出機能がこれを認識します。オプションで、同じ送信元アドレスから繰り返されるポートスキャンを自動的にブロックすることができます。

技術的に言うと、ポートスキャンが検出されるのは、1つの送信元IPアドレスの検出スコアが300ミリ秒の時間枠内で21点を超えたときです。検出スコアは次のように計算されます。

- `1024`未満のTCP宛先ポートに対するスキャン = 3点
- `1024`以上のTCP宛先ポートに対するスキャン = 1点

ポートスキャン検出を有効するには、次の手順に従ってください。

1. ***【ポートスキャン防御(Anti-Portscan)】タブで、【ポートスキャン検出(Portscan Detection)】を有効にします。***
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンが緑色になり、*【グローバル設定(Global Settings)】*エリアが編集可能になります。

2. **次の設定を行います。**
   アクション(Action): 次のアクションを使用できます。

   - **イベントのログのみ(Log Event Only)**: ポートスキャンに対する対策は行われません。イベントのログが記録されるだけです。
   - **トラフィックのドロップ(Drop Traffic)**: さらなるポートスキャンパケットは、ユーザに通知することなくドロップされます。ポートスキャナは、これらのポートがフィルタされたことを報告します。
   - **トラフィックの拒否(Reject Traffic)**: さらなるポートスキャンパケットはドロップされ、ICMP「destination unreachable/port unreachable(宛先到達不可/ポート到達不可)」応答が送信者に送られます。ポートスキャナは、これらのポートがクローズされたことを報告します。

   ログを制限(Limit Logging): ログメッセージの数を抑えたい場合に、このオプションを有効にします。ポートスキャン検出機能は、ポートスキャンが実行されているときに大量のログを生成します。たとえば、ポートスキャンに使用されていると見なされるそれぞれのSYNパケットに対して、ファイアウォールログにエントリが1つ生成されます。このオプションを選択すると、ログが1秒あたり5行までに制限されます。

3. ***【適用(Apply)】をクリックします。***
   設定が保存されます。

8.3.5除外

【ネットワークセキュリティ(Network Security)】>>*【侵入防御(Intrusion Prevention)】*>>*【除外(Exceptions)】*タブでは、侵入防止から除外する送信元ネットワークと宛先ネットワークを定義することができます。

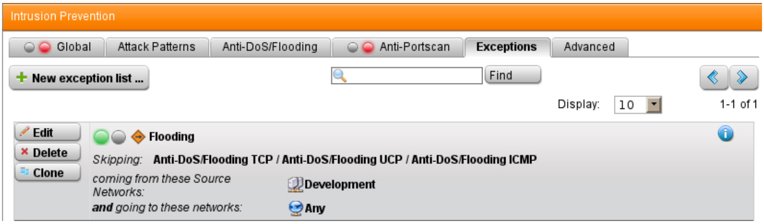


図74 IPS: 除外リスト

除外ルールを作成するには、次の手順に従います。

1. **【除外(Exception)】タブで、【新規除外リスト(New Exception List)】をクリックします。**【除外リストを作成(*Create Exception List*)】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): この除外を説明する名前を入力します。

   スキップするチェック(Skip These Checks): スキップするセキュリティチェックを選択します。

   - **侵入防御(Intrusion Prevention)**: このオプションを選択すると、Astaro Security GatewayのIPSが無効になります。
   - **アンチポートスキャン(Anti-Portscan)**: このオプションを選択すると、ネットワークホストでオープンポートを探すことを目的とする攻撃からの防御が無効になります。
   - **TCP DoS/フラッド防御(Anti-DoS/Flooding TCP)**: 選択すると、TCPSYNフラッド攻撃からの防御が無効になります。
   - **UDP DoS/フラッド防御(Anti-DoS/Flooding UDP)**: 選択すると、UDPフラッド攻撃からの防御が無効になります。
   - **ICMP DoS/フラッド防御(Anti-DoS/Flooding ICMP)**: 選択すると、ICMPフラッド攻撃からの防御が無効になります。

   全リクエストに適用(For All Requests): セキュリティチェックをスキップする条件を少なくとも1つ選択します。条件の前にあるドロップダウンリストで【*And*】または【*Or*】を選択して、複数の条件を論理的に組み合わせることができます。次の条件を設定できます。

   - **送信元ホスト/ネットワークで除外(Coming from These Source Networks)**: 選択して、この除外ルールのセキュリティチェックから除外する送信元ホスト/ネットワークを追加します。条件を選択すると【*ホスト/ネットワーク(Hosts/Networks)*】ダイアログボックスが開くので、各ホストまたはネットワークを入力します。

- **除外するサービス(Using These Services)**: 選択して、この除外ルールのセキュリティチェックから除外するサービスを追加します。条件を選択すると【*サービス(Services)*】ダイアログボックスが開くので、各サービスを追加します。
- **除外する宛先(Going to These Destinations)**: 選択して、この除外ルールのセキュリティチェックから除外するホスト/ネットワークを追加します。条件を選択すると【*宛先(Destinations)*】ダイアログボックスが開くので、各ホストまたはネットワークを入力します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**新しい除外が【*除外(Exceptions)*】リストに表示されます。

例外を編集または削除するには、対応するボタンをクリックします。

注 - ゲートウェイの宛先アドレスを持つパケットに対する侵入防御を除外したい場合、【*宛先(Destinations)*】で【*すべて(Any)*】を選択すると成功しません。ゲートウェイの内部アドレスに対する侵入防御を除外したい場合には、代わりに、【*内部(アドレス)(Internal(Address))*】など、ゲートウェイのIPアドレスが含まれるゲートウェイのインタフェース定義を選択する必要があります。

8.3.6詳細

【*ネットワークセキュリティ(Network Security)*】>>【*侵入防御(Intrusion Prevention)*】>>【*詳細(Advanced)*】タブでは、各IPSルールを手動で変更し、攻撃パターングループから取得されるデフォルトポリシを上書きできます。熟練ユーザのみが設定してください。

変更したルールを作成するには、次の手順に従います。

1. **【*変更されたルール(Modified Rules)*】ボックスで、「+」アイコンをクリックします。**
【*ルールの変更(Modify Rule)*】ダイアログボックスが開きます。
2. **次の設定を行います。**
ルールID(Rule ID): 変更したいルールのIDを入力します。ルールIDを検索するには、AstaroのWebサイトでIPSルールのリストにアクセスします(HTML形式とXML形式の両方が用意されています)。さらに、IPSログまたはIPSレポートでも決定できます。

   このルールを無効化(Disable this Rule): このオプションを選択すると、該当IDのルールが無効になります。

   選択*しない*場合、次の2つのオプションを使用できます。

- **通知の無効化(Disable Notifications)**: このオプションを選択すると、当該ルールが適用された場合に通知がもたらされません。
- **アクション(Action)**: 各ルールが関連付けられるアクション。次のアクションを選択できます。
  - **破棄(Drop)**: 攻撃の疑いがある試行が見つかると、その原因であるデータパケットはドロップされます。
  - **警告(Alert)**:【*破棄(Drop)*】設定と違い、重大なデータパケットはゲートウェイを通過できますが、IPSログにアラートメッセージが記述されます。

3. ***【保存(Save)】をクリックします。***
   【*変更されたルール(Modified Rules)*】ボックスにルールが表示されます。変更を確定するためには、ページの一番下にある【*適用(Apply)*】をクリックする必要もあります。

注 -【*変更されたルール(Modified Rules)*】ボックスにルールIDを追加し、アクションを【*警告(Alert)*】に設定した場合、この変更が有効になるのは、ルールが属するグループが【*攻撃パターン(Attack Patterns)*】タブで有効になっている場合のみです。該当する攻撃パターングループが無効になっている場合、各IPSルールへの変更は効果がありません。

パフォーマンスチューニング

さらに、侵入防御システムのパフォーマンスを向上し、誤検出による警告を最低限に抑えるために、IPSルールの範囲を内部サーバの一部に制限することができます。たとえば、【*攻撃パターン(Attack Patterns)*】タブで【*HTTPサーバ(HTTP Servers)*】グループを有効にし、特定のHTTPサーバをここで選択したとします。この場合、侵入防御システムがHTTPサーバへの攻撃を認識しても、関連付けられたアクション(【*ドロップ(Drop)*】または【*アラート(Alert)*】)は、影響を受けるサーバのIPアドレスとここで選択されたHTTPサーバのIPアドレスが一致する場合に限り、適用されます。

次のサーバタイプに対して、IPSルールの範囲を制限できます。

- **HTTP**: *HTTPサーバ*に含まれるすべての攻撃パターングループ
- **DNS**: 攻撃パターングループ*DNS*
- **SMTP**: 攻撃パターングループ*Exchange*および*Sendmail*
- **SQL**: *データベースサーバ*に含まれるすべての攻撃パターングループ

8.4サーバロードバランシング

サーバロードバランシング機能により、受信接続(例:SMTP、またはHTTPトラフィック)をゲートウェイの背後の複数サーバに分散できます。負荷分散は、送信元IPアドレスに基づいて、1時間持続して行われます。同じ送信元IP IPアドレスからの2つの要求の間隔がこの間隔を超えると、負荷分散は再決定されます。トラフィックの分散は単純なラウンドロビンアルゴリズムに基づいています。

サーバプールのすべてのサーバはICMP ping、TCP接続の確立、またはHTTP/S要求により監視されます。障害が発生すると、影響を受けたサーバは負荷分散に使用されなくなり、問題と考えられる送信元IPの持続性は却下されます。

注 - HTTP/S要求のリターンコードは`1xx Informational`、`2xx Success`、`3xx Redirection`、または`4xx Client Error`のいずれかであることが必要です。その他のすべてのリターンコードは障害の発生を意味します。

8.4.1負荷分散ルール

*【ネットワークセキュリティ(Network Security)】>>【サーバロードバランシング(Server Load Balancing)】>>【負荷分散ルール(Balancing Rules)】*タブで、Astaro Security Gatewayソフトウェアの負荷分散ルールを作成できます。ルールの作成後、サーバ間での重み分散を追加で定義し、インタフェースパーシスタンスを設定することができます。

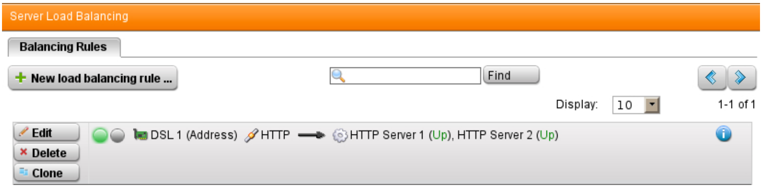


図75 サーバロードバランシング:負荷分散ルールリスト

負荷分散のルールを作成するには、以下の手順に従います。

1. ***【負荷分散ルール(Balancing Rules)】タブで、【新規負荷分散ルール(New Load Balancing Rule)】をクリックします。***
   *【新規負荷分散ルールの作成(Create New Load Balancing Rule)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
サービス(Service): 負荷分散するネットワークサービスを選択します。

仮想サーバ(Virtual Server): 受信トラフィックの元のターゲットホスト。このアドレスは通常、ゲートウェイの外部アドレスと同じになります。

実際のサーバ(Real Servers): 交替でサービスのトラフィックを受け付けるホスト。

チェックタイプ(Check Type): サービスモニタリング用に【*TCP*】(TCP接続の確立)、【*UDP*】(UDP接続の確立)、【*Ping*】(ICMP Ping)、【*HTTPホスト(HTTP Host)*】(HTTP要求)、または【*HTTPSホスト(HTTPS Hosts)*】(HTTPS要求)のいずれかを選択します。【*UDP*】を使用する場合、ping要求が最初に送信され、成功した場合は、続いてペイロード0のUDPパケットが送信されます。pingが成功しなかった場合や、ICMPポートに到達できない場合、このサーバはダウンしているとみなされます。*HTTP*および*HTTPS*要求の場合は、【*URLのチェック(Check URL)*】を入力します。ホスト名は指定してもしなくても構いません(例:`index.html`あるいは`www.example.com/index.html`)。

チェック間隔(Check Interval): チェック間隔を秒単位で入力します。デフォルトは15秒です。つまり、15秒ごとに、実際の全サーバの健全性状態がチェックされます。

自動ファイアウォールルール(Automatic Firewall Rules)(オプション):このチェックボックスは、ゲートウェイルールを自動生成する場合に選択します。これらのルールにより、トラフィックをホストから実際のサーバに送ることができます。

仮想サーバアドレスのシャットダウン(Shutdown Virtual Server Address)(オプション):このチェックボックスは、追加のアドレスを負荷分散用の仮想サーバとして使用する場合(「追加アドレス」の章を参照)にのみ使用できます。すべてのリアルサーバが利用不可になった場合、追加アドレスインタフェースは自動的にシャットダウンされます。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
新しいルールは【*負荷分散(Balancing Rules)*】リストに表示されます。これはデフォルトで無効になっています(ステータスアイコンは赤)。

4. **負荷分散ルールを有効にします。**
ルールを有効にするには、ステータスアイコンをクリックします。

ステータスアイコンが緑色に変わります。

負荷分散ルールを編集または削除するには、該当するボタンをクリックします。

例：それぞれ`192.168.66.10`および`192.168.66.20`というIPアドレスの2台のHTTPサーバがDMZにあるとします。ゲートウェイの外部インタフェースで受信したHTTPトラフィックを両方のサーバに均等に分散したいと仮定します。負荷分散ルールをセットアップするには、各サーバのホスト定義を選択あるいは作成します。それらを*http_server_1*および*http_server_2*とします。次に、【*新規負荷分散ルールの作成(Create New Load Balancing Rule)*】ダイアログボックスで、【*サービス(Service)*】として【*HTTP*】を選択します。さらに、【*仮想サーバ(Virtual Server)*】としてゲートウェイの外部アドレスを選択します。最後に、【*実際のサーバ(Real Servers)*】ボックスにホスト定義を入力します。

重み分散およびインタフェースパーシスタンス

負荷分散サーバ間で重みを分散し、それらの間にインタフェースパーシスタンス設定するには、以下の手順に従ってください。

1. **負荷分散ルールの【*編集(Edit)*】ボタンをクリックします。**
   【*負荷分散ルールの編集(Edit Load Balancing Rule)*】ダイアログボックスが開きます。

2. **【*リアルサーバ(Real Servers)*】ボックスのヘッダで【スケジューラ(Scheduler)】ボタンをクリックします。**
   【*スケジューラの編集(Edit Scheduler)*】ダイアログボックスが開きます。

3. **次の設定を行います。**
   加重(Weight)：加重とは、あるサーバが処理するトラフィック量を他のサーバに対して相対的に示すもので、0～100の間で設定できます。加重ラウンドロビンアルゴリズムが使用され、値が大きいほど、該当サーバにルーティングされるトラフィックが多くなります。相対的な値であるため、合計して100にする必要はありません。たとえば、サーバ1の値を100に、サーバ2の値を50に、サーバ3の値を0に設定することなどができます。この場合、サーバ2のトラフィック量はサーバ1の半分となり、サーバ3は他のサーバが使用可能でない場合にのみ使用されます。0の値は、より値が大きい他のサーバが常に使用されることを示します(他のインタフェースが使用可能であれば)。

   パーシステンス(Itf. Persistence:)：インタフェースパーシスタンスとは、クライアントからの後続の接続が常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間です。この負荷分散ルールのインタフェースパーシスタンスを無効化することもできます。

4. **【*保存(Save)*】をクリックします。**
   【*スケジューラの編集(Edit Scheduler)*】ダイアログボックスが終了し、設定が保存されます。

5. **【保存(*Save*)】をクリックします。**
   【*負荷分散ルールの編集(Edit Load Balancing Rule)*】ダイアログボックスが閉じます。

8.5VoIP

VoIP(*Voice over Internet Protocol*)は、インターネットまたは他のIPベースのネットワークを通した音声会話のルーティングです。Astaro Security Gateway は、IPネットワーク上で音声信号を伝送するために最もよく使用される次のプロトコルのサポートを提供しています。

- SIP
- H.323

8.5.1SIP

Session Initiation Protocol(SIP)は2つ以上の通信パートナー間のセッションの設定、変更、および終了のための信号を送るプロトコルです。SIPは主に音声または音声通話の確立と終了処理に使用します。SIPはTCPをポート`5060`で使用して、コール設定時にエンドポイント間で使用する動的ポート範囲をネゴシエートします。動的範囲内のすべてのポートを開くとセキュリティに重大な問題が生じるため、ゲートウェイでSIPトラフィックをインテリジェントに処理することができます。これは、特別なコネクショントラッキングヘルパによって実現します。このヘルパは制御チャネルをモニタリングし、どの動的ポートが現在使用されているかを判断して、制御チャネルがビジーであるときはこれらのポートのみをトラフィックが通過するようにします。これを行うために、SIPプロトコルを介した通信を可能にする適切なファイアウォールルールを作成するために、SIPサーバとクライアントネットワーク定義の両方を指定する必要があります。

図76 VoIP SIP: VoIP SIPの有効化

SIPプロトコルのサポートを有効にするには、以下の手順に従います。

1. ***【SIP】*タブで、SIPプロトコルのサポートを有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり*【グローバルSIP設定(Global SIP Settings)】*エリアが編集可能になります。

2. **次の設定を行います。**
   SIPサーバネットワーク(SIP Server Networks): ここで、SIPクライアントの接続先として許可されるSIPサーバ(ISPが提供)を選択します。セキュリティ上の理由から、*【すべて(Any)】*は選択しないでください。

   SIPクライアントネットワーク(SIP Client Networks): SIP通信の開始や応答を許可されるSIPクライアントのホスト/ネットワークを選択します。SIPクライアントとはLAN内のエンドポイントであり、他のSIPクライアントとのリアルタイムな双方向通信に関与します。

   厳格モードの有効化(Enable Strict Mode)(オプション): セキュリティを強化するには、このオプションを選択します。ただし、ISPとの接続で問題が発生する場合は、厳格モードを無効にしてください。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

設定をキャンセルするには、*【有効化を中止(Abort Enable)】*またはアンバー色のステータスアイコンをクリックします。

8.5.2H.323

H.323とは、ITU-T(*国際電気通信連合*)が公開した国際マルチメディア通信プロトコル標準であり、あらゆるパケット交換網上で音声・映像通信セッションを提供するプロトコルを規定しています。H.323は、VoIP(*ボイスオーバーIP*)やIPベースのテレビ会議で一般的に使用されます。

H.323では、ポート1720でTCPを使用して、エンドポイント間で使用する動的ポート範囲をコールのセットアップ時にネゴシエートします。動的範囲内ですべてのポートを開くと、セキュリティ上で重大な問題が発生するため、ゲートウェイはインテリジェントベースでH.323関連のトラフィックを許可することができます。これは、特別なコネクショントラッキングヘルパによって実現します。このヘルパは制御チャネルをモニタリングし、どの動的ポートが現在使用されているかを判断して、制御チャネルがビジーであるときはこれらのポートのみをトラフィックが通過するようにします。この目的を達成するためには、H.323プロトコルでの通信を可能にする適切なファイアウォールルールを作成するために、H.323ゲートキーパとクライアントネットワーク定義の両方を指定する必要があります。

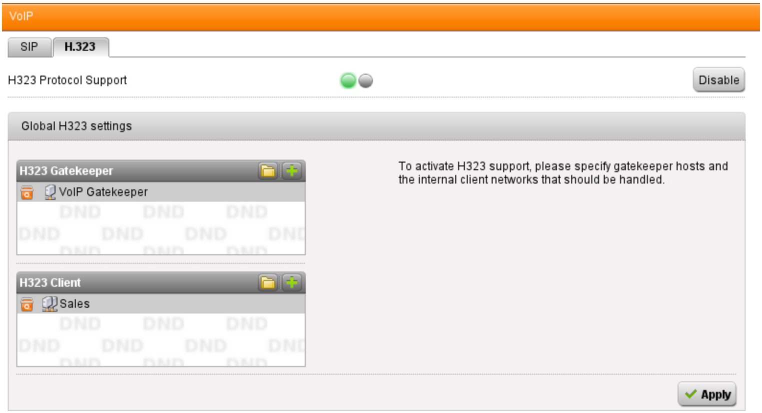


図77 VoIP H.323:VoIP H.323の有効化

H.323プロトコルのサポートを有効にするには、以下の手順に従います。

1. **【*H.323*】タブで、H.323プロトコルのサポートを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色になり、【*グローバルH.323設定(Global H.323 Settings)*】エリアが編集可能になります。

2. **次の設定を行います。**
   H.323ゲートキーパ(H.323 Gatekeeper): H.323ゲートキーパを選択します。H.323ゲートキーパは、ゾーン内のすべてのH.323クライアント(マイクロソフトのNetMeetingなどのエンドポイント)をコントロールします。より具体的には、ゲートキーパはLAN上のゾーン内のすべてのH.323コールに対するモニタとして機能します。ゲートキーパの最重要タスクは、シンボルエイリアスアドレスとIPアドレスとの変換です。

   H.323クライアント(H.323 Client): ここで、H.323接続を開始する元のホスト/ネットワークと宛先のホスト/ネットワークを選択できます。H.323クライアントとはLAN内のエンドポイントであり、他のH.323クライアントとのリアルタイムな双方向通信に関与します。

   厳格モードの有効化(Enable Strict Mode)(オプション):セキュリティを強化するには、このオプションを選択します。ただし、ISPとの接続で問題が発生する場合は、厳格モードを無効にしてください。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

設定をキャンセルするには、*【有効化を中止(Abort Enable)】*またはアンバー色のステータスアイコンをクリックします。

8.6詳細

*【ネットワークセキュリティ(Network Security)】>>【詳細(Advanced)】*メニューのタブを使用すると、ジェネリックプロキシ、SOCKSプロキシ、IDENTリバースプロキシなど追加のネットワークセキュリティ機能を設定することができます。

8.6.1汎用プロキシ

ジェネリックプロキシ(別名「ポートフォワーダ」)は、DNATとマスカレーディングの両機能を組み合わせており、特定のサービスへのすべての受信トラフィックを任意のサーバに転送(フォワーディング)します。標準DNATとの違いは、ジェネリックプロキシでは送信接続についても要求の送信元IPアドレスをインタフェースのIPアドレスに書き換える点です。さらに、宛先(ターゲット)ポート番号も変更することができます。

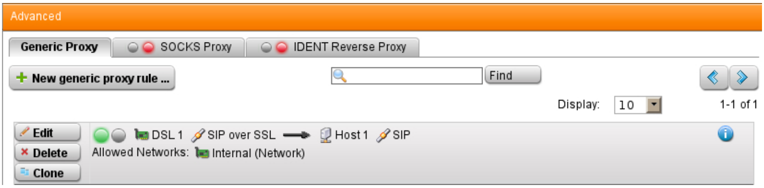


図78 ジェネリックプロキシ：ルールリスト

ジェネリックプロキシルールを追加するには、次の手順に従います。

1. ***【ジェネリックプロキシ(Generic Proxy)】タブで、【新規ジェネリックプロキシルール(New Generic Proxy Rule)】をクリックします。***
   *【新規ジェネリックプロキシルールの作成(Create New Generic Proxy Rule)】*ダイアログボックスが開きます。
2. **次の設定を行います。**
   インタフェース(Interface): 受信接続のインタフェースを選択します。

   サービス(Service): プロキシを使用するトラフィックのサービス定義を選択します。

   ホスト(Host): トラフィックの転送先とするターゲットホストを選択します。

   サービス(Service): プロキシを使用するトラフィックのターゲットサービスを選択します。

   許可ネットワーク(Allowed Networks): ポート転送を適用するネットワークを選択します。

   コメント(Comment)(オプション)：説明などの情報を追加します。
3. ***【保存(Save)】をクリックします。***
   新しいルールが*【ジェネリックプロキシ(Generic Proxy)】*ルールリストに表示されます。
4. **ジェネリックプロキシルールを有効にします。**
   ルールを有効にするには、ステータスアイコンをクリックします。

   これでルールが有効になります(ステータスアイコンは緑)。

ルールを編集または削除するには、対応するボタンをクリックします。

8.6.2SOCKSプロキシ

SOCKS とは、クライアントサーバ型アプリケーションがネットワークファイアウォールのサービスを透過的に使用できるようにするインターネットプロトコルです。ファイアウォール内にある多くのクライアントアプリケーションが、インターネット上のホストと通信するために使用します。例としては、IRC/インスタントメッセージングクライアント、FTPクライアントや、Windows SSH/Telnetクライアントです。フ

ァイアウォールの内側にあるこれらのクライアントは、外側にあるサーバにアクセスしたい場合、その代わりにSOCKSプロキシサーバに接続します。このプロキシサーバは、クライアントが外部サーバにアクセスする適格性をコントロールし、要求をサーバに受け渡します。クライアントアプリケーションは、SOCKS 4またはSOCKS 5というプロトコルバージョンを明示的にサポートしている必要があります。

SOCKSのデフォルトポートは`1080`です。ほぼすべてのクライアントにこのデフォルトポート設定が導入されているため、通常は設定不要です。SOCKSとNATの違いは、SOCKSが「バインド」要求(クライアントの代わりにポートでリスンする機能。わずかなクライアントだけがこれをサポートしています)もサポートしており、SOCKS 5ではユーザ認証が可能である点です。

SOCKSプロキシを有効にする場合、プロキシへのアクセス権がある1つ以上のネットワークを定義しなければなりません。ユーザ認証が必要である場合、SOCKSプロキシの使用を許可するユーザまたはグループも選択する必要があります。

> **注 -** ユーザ認証を使用しない場合、SOCKSプロキシはSOCKS 4プロトコルとSOCKS 5プロトコルの両方で使用できます。ユーザ認証を選択した場合、SOCKS 5のみが機能します。プロキシにSOCKS 5モードでホスト名を解決させる場合、DNSプロキシも有効にする必要があります。有効にしないと、DNS解決は失敗します。

SOCKSプロキシを設定するには、次の手順に従ってください。

1. **【*SOCKSプロキシ(SOCKS Proxy)*】タブで、SOCKSプロキシを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンが緑色になり、【*SOCKSプロキシオプション(SOCKS Proxy Options)*】エリアが編集可能になります。

2. **次の設定を行います。**
   許可ネットワーク(Allowed Networks): SOCKSプロキシの使用を許可するネットワークを選択します。

   ユーザ認証を有効にする(Enable User Authentication): このオプションを選択すると、ユーザはSOCKSプロキシへのログイン時にユーザ名とパスワードを入力しなければならなくなります。ユーザ認証をサポートしているのがSOCKS 5のみであるため、SOCKS 4は自動的に無効になります。

   許可されたユーザ(Allowed Users): SOCKSプロキシの使用を許可するユーザまたはグループを選択します。

3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

8.6.3IDENTリバースプロキシ

IDENTプロトコルは、リモートサーバがアクセス元クライアントの身元を簡単に確認するために使用します。IDENTプロトコルは暗号化されず、スプーフィングが簡単ですが、多くのサービスではいまだにこのプロトコルを使用しており、場合によっては必須です。

IDENTリレーを設定するには、次の手順に従ってください。

1. ***【IDENTリバースプロキシ(IDENT Reverse Proxy)】*タブで、IDENTリレーを有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンが緑色になり、*【グローバル設定(Global Settings)】*エリアが編集可能になります。

2. **次の設定を行います。**
   内部ホストへの転送(Forward to Internal Hosts)(オプション):IDENTクエリはゲートウェイの接続追跡でカバーされないため、マスカレーディングが使用されている場合は「スタック」します。ゲートウェイの内側にあるマスカレーディングされたホストにIDENTクエリを受け渡すためには、*【内部ホストへの転送(Forward to Internal Hosts)】*オプションを選択します。実際のIP接続は転送されません。代わりに、ゲートウェイが内部クライアントにIDENT応答を要求し、その文字列を要求元サーバに転送します。この方法は、主要IRCクライアントとFTPクライアントに組み込まれた大部分の「ミニIDENT」サーバで機能します。

   デフォルト応答(Default Response): IDENTリレーを有効にすると、ゲートウェイはIDENT要求への応答をサポートします。システムは、接続を開始したローカルサービスを問わず常に、*【デフォルト応答(Default Response)】*ボックスに入力した文字列で応答します。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

9 Webセキュリティ

この章では、当製品の基本的はWebセキュリティ機能を設定する方法を説明します。Astaro Security Gateway.

この章には次のトピックが含まれます。

- Webフィルタリング
- Webフィルタプロファイル
- アプリケーションコントロール
- FTPプロキシ

Webadminの【*ウェブセキュリティ統計(Web Security Statistics)*】ページには、時間、トラフィック、ならびに上位ユーザのサーフィンに基づいた最もサーフィンの多いドメインの概要が表示されます。さらに、ブロックされた上位Webサイトカテゴリが表示されます。各セクションには、【*詳細(Detail)*】リンクが含まれています。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

注 - 収集されるWebサーフィンデータはセッションベースです。近似値を得るために、上位ドメインおよびユーザのすべてのデータが以下のように収集されます。各Web要求は、トラフィック量および要求間隔を考慮に入れてログされます。5分間アクティビティがなく、ユーザあるいはドメインに対する要求が記録されないと、そのセッションは終了したものとみなされます。5分間アクティビティがない場合でもユーザがまだWebページを表示している可能性を考えて、【*経過時間(Time Spent)*】の値には常に1分余計に追加されます。レポーティングデータは15分ごとに更新されます。
クライアントが無効なURLを要求した場合、Webフィルタはその要求をログしますが、その要求に応えることはできません。これらのリンクは【*ウェブセキュリティ統計(Web Security Statistics)*】ページでエラーとして計上されます。これらはレポーティングやWebフィルタのエラーではなく、ほとんどの場合、ページ作成者がWebコンテンツに無効または不正なリンクを配置したために発生します。

9.1 Webフィルタリング

【Webセキュリティ(Web Security)】>>【Webフィルタリング(Web Filtering)】メニューのタブを使用すると、Astaro Security GatewayソフトウェアをHTTP/Sキャッシングプロキシとして設定することができます。Astaro Security GatewayのHTTP/Sプロキシは、シンプルなキャッシングに加え、HTTP/Sの使用が許可されているネットワークに対して豊富なWebフィルタ技術を提供しています。これには、シグニチャデータベースとスパイウェアフィルタリング技術が定期的に更新される2つの異なるウイルススキャンエンジンを使用したウイルスおよびスパイウェア感染の防御機能もあり、受信トラフィックと送信トラフィックの両方を保護します。さらに、Astaro Security Gatewayでは、高度なWebサイト分類を採用しており、世界最大のリアルタイムURLデータベースを使用してさまざまなWebページへのアクセスをコントロールできます。

9.1.1 グローバル

【Webセキュリティ(Web Security)】>>【Webフィルタリング(Web Filtering)】>>【グローバル(Global)】タブでは、Webフィルタのグローバル設定を実行できます。

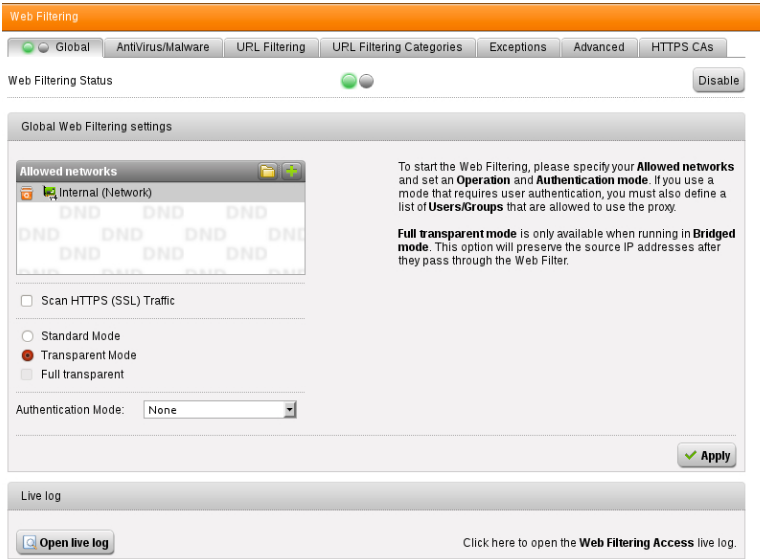


図79 Webフィルタ(Web Filter):グローバル設定

Webフィルタを設定するには、次の手順に従ってください。

1. ***【グローバル(Global)】*タブで、Webフィルタを有効にします。**
ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンが緑色になり、*【グローバルHTTP設定(Global HTTP Settings)】*エリアが編集可能になります。

2. **許可するネットワークを選択します。**
Webフィルタの使用を許可するネットワークを選択します。デフォルトで、WebフィルタはクライアントAント要求をTCPポート8080でリスンし、*【許可ネットワーク(Allowed Networks)】*ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。

3. **HTTPS(SSL)トラフィックのスキャン(Scan HTTPS(SSL)Traffic)**:
HTTPトラフィックに加えHTTPSトラフィックもスキャンする場合は、このチェックボックスにチェックを入れます。

4. **オペレーションのモードを選択します。**
ユーザ認証が必要なオペレーションモードを選択する場合には、Webフィルタの使用を許可するユーザとグループを選択する必要があります。次のオペレーションモードを使用できます。

   - **標準(Standard)**: 標準モードでは、Webフィルタはデフォルトでクライアント要求をポート8080でリスンし、*【許可ネットワーク(Allowed Network)】*ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。
   認証モードを選択します。

     - **なし(None)**: 認証をしない場合に選択します。

     - **Active Directory SSO**:*【定義およびユーザ(Definitions & Users)】>>【認証サーバ(Authentication Servers)】>>【サーバ(Servers)】*タブで*Active Directoryシングルサインオン*(SSO)を設定した場合、これを選択します。これにより、NTLMユーザ認証が認証クライアントで使用されます。動作が保証されるのはInternet Explorerのみです。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。*【ユーザ/グループ(Users/Groups)】*テキストボックスで、Webフィルタの使用を許可するユーザやグループを選択または追加できます。

     - **エージェント(Agent)**: Astaro Authentication Agent(AAA)を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。*【ユーザ/グループ(Users/Groups)】*テキストボッ

クスで、Webフィルタの使用を許可するユーザやグループを選択または追加できます。

- **Apple OpenDirectory SSO**:*【定義およびユーザ(Definitions & Users)】>>【認証サーバ(Authentication Servers)】>>【サーバ(Servers)】*タブで*LDAP*を設定しており、Apple OpenDirectoryを使用している場合、これを選択します。さらに、Webフィルタが正しく機能するようにするためには、*【Webセキュリティ(Web Security)】>>【Webフィルタリング(Web Filtering)】>>【詳細(Advanced)】*タブで、MAC OS Xシングルサインオン Kerberos鍵ファイルをアップロードする必要があります。Webフィルタをこのモードで使用する場合、クライアントはブラウザ設定でWebフィルタを指定しておく必要があります。*【ユーザ/グループ(Users/Groups)】*テキストボックスで、Webフィルタの使用を許可するユーザやグループを選択または追加できます。Safariブラウザは SSOをサポートしていません。

- **基本ユーザ認証(Basic User Authentication)**: このモードでは、各クライアントはWebフィルタを使用する前にこのWebフィルタに対して自己認証する必要があります。サポートされる認証方式について詳しくは、*「定義およびユーザ」>>「認証」*を参照してください。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。*【ユーザ/グループ(Users/Groups)】*テキストボックスで、Webフィルタの使用を許可するユーザやグループを選択または追加できます。

- **eDirectory SSO**:*【定義およびユーザ(Definitions & Users)】>>【認証サーバ(Authentication Servers)】>>【サーバ(Servers)】*タブで*eDirectory*を設定した場合、これを選択します。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。*【ユーザ/グループ(Users/Groups)】*テキストボックスで、Webフィルタの使用を許可するユーザやグループを選択または追加できます。

注 - eDirectoryおよびActive Directoryのシングルサインオン(SSO)モードの場合、Webフィルタはアクセス先のIPアドレスと資格情報を最大15分間キャッシュします。Apple OpenDirectory SSOの場合、キャッシュできるのはグループ情報のみです。これは、認証サーバへの負荷を軽減するために行われます。逆に言うと、ユーザ、グループ、またはアクセスしているユーザのログインステータスの変更がWebフィルタによって反映されるまで、最大15分かかります。

- **透過(Transparent)**: 透過モードでは、ポート80(SSLを使用している場合はポート443)でクライアントブラウザアプリケーションが行うすべての接続はインターセプトされ、クライアント側の設定なしでWebフィルタにリダイレクトされます。クライアントがWebフィルタサーバを意識することは全くありません。このモードの利点は、追加の管理やクライアント側での設定が不要であることで、短所は、処理できるのがHTTP(ポート80)要求のみであることです。そのため、*透過*モードを選択すると、クライアントのプロキシ設定は無効になります。

  フル透過モード(Full Transparent Mode)(オプション): クライアントの送信元IPをゲートウェイのIPに置き換えず、そのまま維持する場合は、【*完全透過モード(Full Transparent Mode)*】チェックボックスにチェックを入れます。これは、クライアントがパブリックIPアドレスを使用しており、Webフィルタによって隠すべきではない場合に便利です。このオプションはブリッジモードのみで意味があるため、ブリッジモードでしか利用できません。

注 - 透過モードでは、WebフィルタはHTTP要求からNTLM認証ヘッダを削除します。さらに、WebフィルタはこのモードではFTP要求を処理できません。クライアントがこのようなサービスにアクセスする必要がある場合は、ファイアウォールでポート(21)を開く必要があります。一部のWebサーバは、ポート80以外のポート経由でストリーミング動画や音声などのデータを送信します。これらの要求は、Webフィルタが透過モードで機能しているときは検知されません。このようなトラフィックにも対応したい場合には、他のモードを使用するか、これらを許可する明確なファイアウォールルールを入力する必要があります。

認証モードを選択します。

- **なし(None)**: 認証をしない場合に選択します。
- **エージェント(Agent)**: Astaro Authentication Agent(AAA)を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。【*ユーザ/グループ(Users/Groups)*】テキストボックスで、Webフィルタの使用を許可するユーザやグループを選択または追加できます。
- **ブラウザ**: 選択すると、Webフィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます。

5. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

重要 - SSLスキャニングを透過モードと組み合わせて有効にすると、一部のSSL接続(SSL VPNトンネルなど)が失敗します。SSL VPN接続を有効にするには、対応するターゲットホストを*【透過モードスキップリスト(Transparent Mode Skiplist)】*に追加します(*「Webセキュリティ」>>「Webフィルタリング」>>「詳細」*を参照)。

9.1.2アンチウイルス/マルウェア

*【Webセキュリティ(Web Security)】>>【Webフィルタリング(Web Filtering)】>>【アンチウイルス/マルウェア(AntiVirus/Malware)】*タブでは、ウイルス、ワーム、その他のマルウェアといった有害で危険なコンテンツを伝送するWebトラフィックからネットワークを保護することを目的とするオプションを設定することができます。

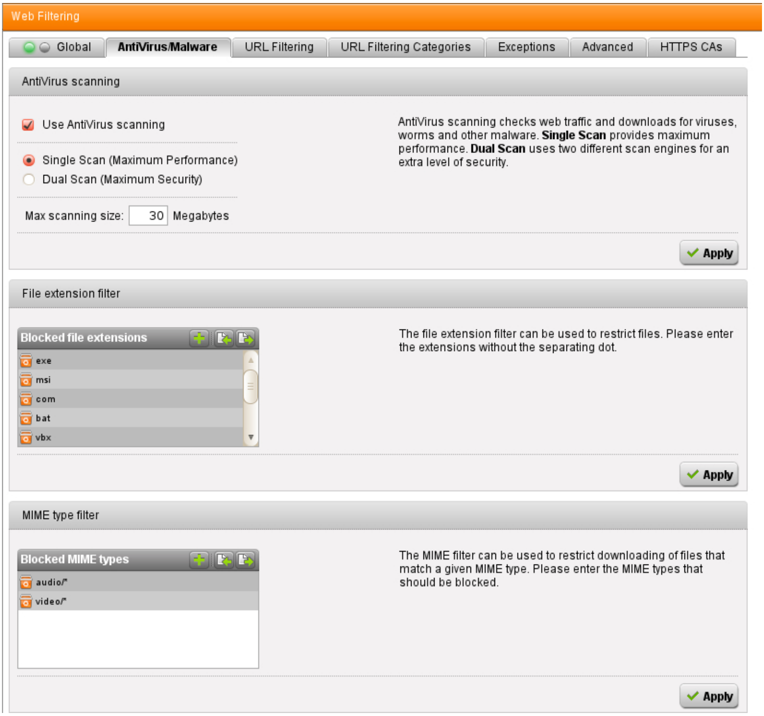


図80 Webフィルタ(Web Filter):アンチウイルス/マルウェア設定の構成

アンチウイルススキャン(AntiVirus Scanning)

送信および受信Webトラフィックをスキャンするためには、【*アンチウイルススキャンを使用(Use AntiVirus Scanning)*】オプションを選択します。Astaro Security Gatewayは、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン(Single Scan)**: デフォルトの設定で、最高のパフォーマンスを提供します。
- **デュアルスキャン(Dual Scan)**: すべてのWebトラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、認識率を最大限に高めます。

最大スキャンサイズ(Max Scanning Size): アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

設定を保存するには【*適用(Apply)*】をクリックします。

ファイル拡張子フィルタ(File Extension Filter)

この機能では、ファイルの拡張子(実行可能バイナリなど)に基づいて、【*ブロックするファイル拡張子(Blocked File Extensions)*】ボックスにファイル拡張子がリストされている特定のタイプのファイルをWebトラフィックからフィルタします。ファイル拡張子を追加したり、ブロック対象から外すファイル拡張子を削除したりすることができます。ファイル拡張子を追加するには、【*ブロックするファイル拡張子(Blocked File Extensions)*】ボックスの「+」アイコンをクリックし、ブロックしたいファイル拡張子(`exe`など)を入力します。区切り文字のドットは不要です。

設定を保存するには【*適用(Apply)*】をクリックします。

注 - 暗号化された`zip`アーカイブは、悪意あるコンテンツについてスキャンすることはできず、ウイルススキャナを通過します。暗号化された`zip`ファイルに含まれるマルウェアからネットワークを保護するために、`zip`ファイル拡張子をすべてブロックすることを検討してください。

MIMEタイプフィルタ(MIME Type Filter)

ブロックするMIMEタイプを追加するには、【*ブロックするMIMEタイプ(Blocked MIME Types)*】ボックスの「+」アイコンをクリックし、MIMEタイプを入力します(`image/gif`など)。ここではワイルドカード(*)を使用できます(`audio/*`など)。

アクティブコンテンツ削除(Active Content Removal)

【*アクティブコンテンツ削除(Active Content Removal)*】エリアでは、Webページに埋め込まれたオブジェクト(例:マルチメディアファイル)など特定のWebコンテンツが自動的に削除されるように設定することができます。次の設定が可能です。

- **埋め込みオブジェクトの削除(Remove Embedded Objects)**: 選択すると、この機能はすべての<OBJECT>タグをHTMLページから削除し、ActiveX、Flash、Javaなどの動的コンテンツを受信HTTPトラフィックから除去します。
- **JavaScriptの無効化(Disable JavaScript)**: 選択すると、この機能はHTMLページ内のすべての<SCRIPT>タグを無効にするため、HTMLページに埋め込まれた機能やインクルードされた機能が無効になります。

9.1.3URLフィルタリング

*【Webセキュリティ(Web Security)】>>【Webフィルタリング(Web Filtering)】>>【URLフィルタリング(URL Filtering)】*タブでは、特定の種類のWebサイトに対するアクセスをコントロールするデフォルト設定を構成できます。

注 - 常に、ホワイトリストに対する照会が先に行われます。つまり、各Webサイトリクエストをホワイトリストと比較して、一致が見つからなかった場合、ブラックリストと比較します。ブラックリストとの一致が見つかると、Webサイトはブロックされます。

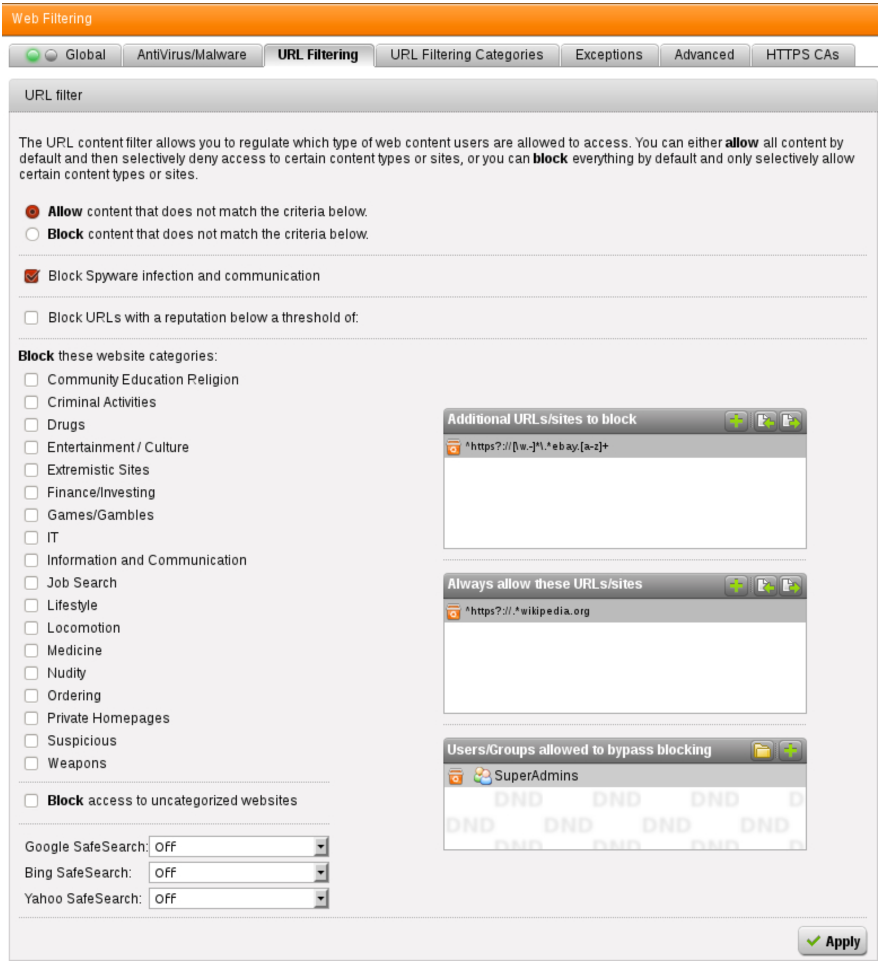


図 81　Webフィルタ(Web Filter) : URLフィルタリングの設定

次の設定が可能です。

- ***選択の許可(Allow)/ブロック(Block)***：選択したWebサイトカテゴリを許可するかブロックするかを決定します。次のオプションを使用できます。
    - **次の条件に一致しないコンテンツを許可(Allow Content that Does not Match the Criteria Below)**：このオプションを選択すると、選択したWebサイトカテゴリはブロックされますが、選択していない他のすべてのカテゴリは許可されま

す。

- **次の条件に一致しないコンテンツをブロック(Block Content that Does not Match the Criteria Below)**: このオプションを選択すると、選択したカテゴリを除くすべてのWebサイトカテゴリがブロックされます。

デフォルトオプションは【*許可(Allow)*】です。【*ブロック(Block)*】に切り替えると、これに従って下のオプションの意味は「逆に」なり、表示されるテキストで「*ブロック(Block)*」が「*許可(Allow)*」に(あるいはその逆に)置き換えられます。

注 - 分類データベースにアクセスするためには、アップストリームのファイアウォールでTCPポート`6000`またはTCPポート`80`を開放する必要があります。親プロキシを設定している場合、データベースへのすべての要求は親プロキシ経由で送信されます。

- **スパイウェアの伝染及び通信をブロック(Block Spyware Infection and Communication)**: スパイウェアとは、ユーザに認識させることなくシステムを精査して、ユーザの行動を広告主に報告する悪意のあるソフトウェアです。このオプションを選択すると、サーバからクライアントへのトラフィックでスパイウェアを検出し、ブロックします。これにより、ネットワーク内のコンピュータが新しいスパイウェアに感染するのを防ぐことができます。さらに、この機能を有効にすると、すでにインストールされているスパイウェアアプリケーションについても検出し、トラフィックをブロックできます。この結果、スパイウェアが収集したユーザ情報がインターネットに送信されなくなります。このオプションは、ページの最初のオプションを【*許可(Allow)*】に設定した場合に限り使用できます。

注 - スパイウェアカテゴリは、使用可能な18グループのいずれにも割り当てることができません。したがって、【*スパイウェアの伝染及び通信をブロック(Block Spyware Infection and Communication)*】チェックボックスにチェックを入れることによってのみ、スパイウェア提供者から防御することができます。

- **しきい値より評判が低いURLをブロック(Block URLs with a Reputation Below a Threshold of)**: Webサイトは「*信頼される(Trusted)*」、「*中立(Neutral)*」、「*疑わしい(Suspicious)*」または「悪意のある」に分類できますが、「悪意のある」はリストされていません(これは、「悪意のある」がリストに含まれていると、該当するすべてのサイトに対してしきい値オプションをまったく使用しないことが許可されてしまうためです)。未分類のWebサイトを「*未確認(Unverified)*」と呼びます。ネットワークからアクセスできるWebサイトがどのような評判を持つべきかを決定することができます。選択したしきい値を下回るWebサイトはブロックされます。このオプションは、ページの最初のオプションを【*許可(Allow)*】に設定した場合に限り使用できます。Webサイトの評判について詳しくは、http://www.trustedsource.orgを参照してください。

- **これらのWebサイトカテゴリをブロック(Block these Website Categories)**: ブロックするWebサイトカテゴリを選択します。ページの最初のオプションを【*ブロック(Block)*】に設定した場合、このオプションは【*これらのWebサイトカテゴリを許可(Allow these Website Categories)*】に変わります。ここで選択するWebサイトカテゴリとその下位のサブカテゴリのマッピングは、【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*URLフィルタリングカテゴリ(URL Filtering Categories)*】タブで変更できます。

> **注 -** Webサイトが正しく分類されていないと思われる場合は、次のURLレポートフォームを使用して新しいカテゴリをご提案いただけます。

- **未分類Webサイトへのアクセスをブロック(URL Filtering Categories)**: このオプションを選択すると、未知のコンテンツを持つWebサイトをブラウザで開けなくなります。この機能は、好ましくないと思われるWebサイトが相応の分類をされていない場合のフォールバックセキュリティメカニズムと考えることができます。
この機能のメリットの1つに、いわゆるフィッシング攻撃からユーザを保護できることがあげられます。一般にフィッシングEメールには、偽造Webサイトへの疑わしいリンクが記載されています。この目的は、ユーザをだまして個人情報や機密情報を提供させることです。まだ有害と分類されていない場合、これらのリンクは「*未分類(Uncategorized)*」または「*疑わしい(Suspicious)*」カテゴリとなります。このオプションを選択すると、これらのカテゴリはブロックされます。これにより、フィッシングメッセージが送信されても、ユーザは偽造URLを開くことができません。
ページの最初のオプションを【*ブロック(Block)*】に設定した場合、このオプションは【*未分類Webサイトへのアクセスを許可(Allow Access to Uncategorized Websites)*】に変わります。

- **ブロックする追加URL/サイト(Additional URLs/Sites to Block)**: 特定のURLまたはWebサイトをカテゴリを問わずブロックしたい場合には、ここに入力します。これにより、ここにリストされたWebサイトを、たとえ許可されるカテゴリに属していてもブロックすることができるという効果があります。ここでは正規表現が許可されます(`^https?://.*wikipedia.org`など)。1つのURLだけをブロックする場合は、URL全体を入力します(`http://www.wikipedia.org`など)。`wikipedia.org`のような表現を使用すると、対象のURLだけではなく、検索結果や類似URLの一部にも一致してしまうため、意図しないブロックにつながる可能性があります。
ページの最初のオプションを【*ブロック(Block)*】に設定した場合、このオプションは【*許可する追加URL/サイト(Additional URLs/Sites to Allow)*】に変わります。

- **常に許可するURL/サイト(Always Allow these URLs/Sites)**: 特定のURLまたはWebサイトを、カテゴリやブロックリストのエントリを問わず明示的に許可したい場合には、ここに入力します。ここでは正規表現が許可されます(`^https?://.*wikipedia.org`な

ど)。1つのURLだけを許可する場合は、URL全体を入力します(`http://www.wikipedia.org`など)。`wikipedia.org`のような表現を使用すると、対象のURLだけではなく、検索結果や類似URLの一部にも一致してしまうため、意図しないブロックにつながる可能性があります。
ページの最初のオプションを【*ブロック(Block)*】に設定した場合、このオプションは【*これらのURL/サイトを常にブロック(Always Block these URLs/Sites)*】に変わります。

- **ブロックのバイパスが許可されるユーザ/グループ(Users/Groups Allowed to Bypass Blocking)**: 特定のユーザまたはグループに対し、デフォルトでブロックされるページへのアクセスを許可する場合には、これらのユーザ/グループをこのドラッグアンドドロップボックスに追加します。これにより、ブロックされるページに【*URLをブロック解除(Unblock URL)*】ボタンが表示されるようになります。このボタンをクリックすると新しいページが開き、ユーザは資格情報およびブロックページへのアクセスを希望する理由を入力できます。このユーザが、直接またはグループ経由でバイパスブロックボックスに含まれていれば、ブロックページにアクセスできるようになります。バイパスはログに記録され、レポートの一部となります(【*ログおよびレポーティング(Logging & Reporting)*】>>【*Webセキュリティ(Web Security)*】>>【*ブロック状況(Blocked Usage)*】を参照)。
- **SafeSearch**: Google、Bing、Yahooの各検索エンジンに対してSafeSearchの使用を強制することができます。SafeSearchフィルタは、子供にふさわしくないコンテンツ(犯罪や不正)を検索結果から削除します。有効にすると、Webフィルタ経由でWebサーフィンをするユーザはフィルタをオフにできません。

9.1.4URLフィルタリングカテゴリ

【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*URLフィルタリングカテゴリ(URL Filtering Categories)*】タブでは、Webサイトカテゴリからカテゴリグループへのマッピングをカスタマイズできます。これは【*URLフィルタリング(URL Filtering)*】タブで選択できます。Astaro Security Gateway は、60種類のWebサイトカテゴリを識別し、アクセスをブロックすることができます。高度なURL分類方法により、疑わしいWebサイトの識別における精度と完全性が保証されます。データベースに含まれていないWebページをユーザが要求すると、URLがWebクローラに送信され、自動的に分類されます。

注 - Webサイトが正しく分類されていないと思われる場合は、次のURLレポートフォームを使用して新しいカテゴリをご提案いただけます。

Webサイトカテゴリをカテゴリグループに割り当てるには、次の手順に従ってください。

1. **編集するカテゴリグループで【*編集(Edit)*】をクリックします。**
   【*フィルタカテゴリの編集(Edit Filter Category)*】ダイアログボックスが開きます。

2. **サブカテゴリを選択します。**
グループに追加(またはグループから削除)するサブカテゴリのチェックボックスにチェックを入れます(またはチェックを外します)。

3. **【*保存(Save)*】をクリックします。**
指定した設定でグループが更新されます。

あるいは、新しいフィルタカテゴリを作成することもできます。次の手順で実行します。

1. **ページ上部にある【*新規フィルタカテゴリ(New Filter Category)*】ボタンをクリックします。**
【*フィルタカテゴリの作成(Create Filter Category)*】ダイアログボックスが開きます。

2. **名前を入力します。**
新しいフィルタカテゴリを説明する名前を入力してください。

3. **サブカテゴリを選択します。**
グループに追加するサブカテゴリのチェックボックスを選択します。

4. **【*保存(Save)*】をクリックします。**
指定した設定でグループが更新されます。

カテゴリを編集または削除するには、対応するボタンをクリックします。

9.1.5除外

【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*除外(Exceptions)*】タブでは、クライアントネットワーク、ユーザ/グループ、ドメインのホワイトリストを定義できます。これらのリストに含まれるすべてのエントリを、特定のWebセキュリティサービスの対象外にすることができます。

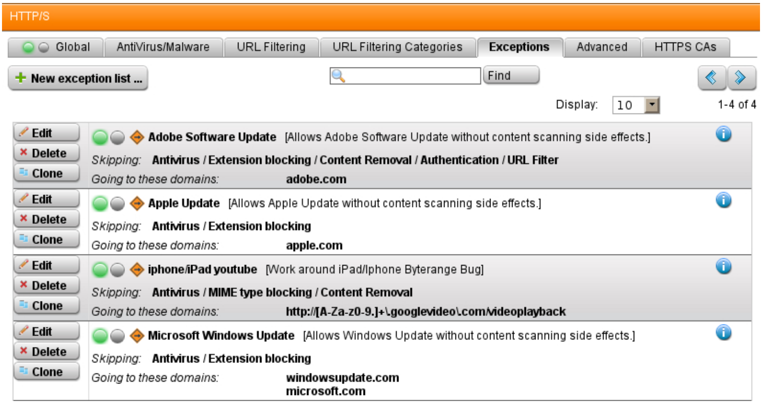


図82 Webフィルタ(Web Filter):除外リスト

除外ルールを作成するには、次の手順に従います。

1. **【除外(Exception)】タブで、【新規除外リスト(New Exception List)】をクリックします。【*除外リストを作成(Create Exception List)*】ダイアログボックスが開きます。**
2. **次の設定を行います。**
   名前(Name): この除外を説明する名前を入力します。

   コメント(Comment)(オプション):説明などの情報を追加します。

   スキップするチェック(Skip These Checks): スキップするセキュリティチェックを選択します。

   - **認証(Authentication)**: Webフィルタを*認証*モードで実行している場合、送信元ホスト/ネットワークまたはターゲットドメインの認証をスキップできます。
   - **キャッシング(Caching)**: 選択すると、特定のドメインまたは送信元ホスト/ネットワークのキャッシングが無効になります。
   - **アンチウイルス(AntiVirus)**: 選択すると、ウイルスやトロイの木馬などの好ましくないコンテンツがメッセージに含まれていないかチェックするウイルススキャンが無効になります。
   - **拡張子ブロック(Extension Blocking)**: 選択すると、ファイル拡張子フィルタが無効になります。このフィルタは、拡張子に基づいて特定タイプのファイルが含まれるコンテンツをブロックするために使用します。

- **MIMEタイプブロック(MIME Type Blocking)**: 選択すると、MIME タイプフィルタが無効になります。このフィルタは、特定のMIMEタイプのコンテンツをブロックするために使用します。
- **URLフィルタ(URL Filter)**: 選択すると、URL フィルタが無効になります。このフィルタは、特定の種類のWebサイトへのアクセスをコントロールします。
- **コンテンツ削除(Content Removal)**: 選択すると、(マルチメディアファイルなどの)埋め込みオブジェクトやJavaScriptといったWebページ内の特殊コンテンツの削除がバイパスされます。
- **SSLスキャン(SSL Scanning)**: 選択すると、要求内のWebページに対するSSLスキャンがスキップされます。これは、オンラインバンキングのWebサイトや、SSLインターセプションがうまく機能しないWebサイトなどで有用です。技術的な理由から、このオプションは透過Webフィルタモードでは機能しません。透過モードでは、代わりに「*透過スキップリスト(Transparent Skiplist)*」を使用してください(「詳細」を参照)。標準モードでは、クライアントが何を送信するのかに応じて、宛先ホストまたはIPアドレスのみに基づいて除外ルールを作成できます。URL全体ではなくカテゴリに基づく除外では、ホスト名のみが分類されます。
- **証明書信頼性チェック(Certificate Trust Check)**: 選択すると、HTTPS サーバ証明書の信頼性チェックがスキップされます。Webフィルタが認証ありの透過モードで機能している場合、ユーザ/グループの照合に基づく証明書の信頼性チェックをスキップすることは技術的に不可能です(*【ユーザ/グループからの全リクエストに適用(For All Requests Coming From These Users/Groups)】*)。
- **証明書日付チェック(Certificate Date Check)**: 選択すると、HTTPS証明書の日付が有効であるかどうかのチェックがスキップされます。

労働協議会のスタッフや会員など、アクティビティをロギングすべきではない人がいる場合には、次の2つのオプションが便利です。

- **アクセスしたページ(Accessed Pages)**: 選択すると、アクセスしたページのログが記録されなくなります。これらのページ要求は、レポートからも除外されます。
- **ブロックされたページ(Blocked Pages)**: 選択すると、ブロックされたページのログが記録されなくなります。これらのページ要求は、レポートからも除外されます。

全リクエストに適用(For All Requests): セキュリティチェックをスキップする条件を少なくとも1つ選択します。条件の前にあるドロップダウンリストで*【And】*または*【Or】*を選択して、複数の条件を論理的に組み合わせることができます。次の条件を設定できます。

- **送信元ホスト/ネットワークで除外(Coming from These Source Networks)**: 選択して、この除外ルールのセキュリティチェックから除外する送信

元ホスト/ネットワークを追加します。条件を選択すると【*ホスト/ネットワーク(Hosts/Networks)*】ダイアログボックスが開くので、各ホストまたはネットワークを入力します。

- **これらのURLと照合(Matching These URLs)**: 選択して、この除外ルールのセキュリティチェックから除外するターゲットドメインを追加します。条件を選択すると【*ターゲットドメイン(Target Domains)*】ダイアログボックスが開くので、各ドメインを追加します。例: `^https?://[^.]*\.domain.com`は、ドメインのすべてのサブドメインへのHTTP(S)接続と一致します。

> **注 -** SSLスキャニングを有効にして*透過*モードを使用している場合、ターゲットドメインをIPアドレスで入力する必要があります。IPアドレスを入力しないと、除外は技術的な理由で失敗します。

- **除外するユーザ/グループ(Coming from These Users/Groups)**: 選択して、この除外ルールのセキュリティチェックから除外するユーザまたはユーザグループを追加します。条件を選択すると【*ユーザ/グループ(Users/Groups)*】ダイアログボックスが開くので、各ユーザまたはグループを入力します。また、標準モードでは認証が存在しないため、特定のユーザ/グループの照合は機能しません。
- **除外するWebサイトカテゴリ(Going to These Categories of Websites)**: 選択すると、特定のカテゴリに対するセキュリティチェックがスキップされます。条件を選択するとリストが開くので、カテゴリを選択します。

3. **【*保存(Save)*】をクリックします。**
   新しい除外が【*除外(Exceptions)*】リストに表示されます。

例外を編集または削除するには、対応するボタンをクリックします。

9.1.6詳細

【*Webセキュリティ(Web Security)*】>>【*Web フィルタリング(Web Filtering)*】>>【*詳細(Advanced)*】タブには、キャッシングやポートの設定など、Webフィルタの各種設定オプションが用意されています。

ストリーミング設定(Streaming Settings)

ストリーミングコンテンツに対するコンテンツスキャンをバイパス(Bypass Content Scanning for Streaming Content): このオプションを選択すると、一般的な音声・動画ストリーミングコンテンツがコンテンツスキャンの対象外となります。このオプションを無効にすると、大部分のメデ

ィアストリームは事実上無効になります。これは、このようなストリームを合理的な時間内でスキャンすることができないためです。そのため、このオプションは選択することを推奨します。

透過モードスキップリスト(Transparent Mode Skiplist)

このオプションは、Webフィルタを透過モードで実行している場合のみ有用です。【*透過モード時にスキップするホスト/ネット(Skip Transparent Mode Hosts/Nets)*】ボックスにリストされているホストとネットワークは、HTTPトラフィックの透過的インターセプションの対象とはなりません。ボックスは、送信元ホスト/ネットワーク用に1つ、宛先ホスト/ネットワーク用に1つあります。これらのホストとネットワークに対して、HTTPトラフィックを(プロキシなしで)許可するには、【*リスト内のホスト/ネットワークのHTTPトラフィックを許可(Allow HTTP Traffic for Listed Hosts/Nets)*】チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

プロキシの自動設定(Proxy Auto Configuration)

プロキシの自動設定とは、ブラウザにフェッチされるプロキシ自動設定ファイル(PACファイル)を一元的に提供するための機能です。ブラウザはこれを受けて、PACファイルに記述された詳細に従ってプロキシ設定を構成します。

PACファイルの名前は*wpad.dat*、MIMEタイプは`application/x-ns-proxy-autoconfig`であり、ASGから提供されるものです。このファイルには、次のように、テキストボックスに入力した情報が含まれています。

```
function FindProxyForURL(url, host)
 { return "PROXY proxy.example.com:8080; DIRECT"; }
```

上の関数は、すべてのページ要求をポート`8080`上の`proxy.example.com`というサーバのプロキシにリダイレクトするようブラウザに指示しています。プロキシに到達できなければ、インターネットへの直接接続が確立されます。

ネットワークでPACファイルを提供するには、次の方法があります。

- ブラウザ設定経由で提供する:【*プロキシ自動設定の有効化(Enable Proxy Auto Configuration)*】オプションを選択すると、ASG Web フィルタ経由でPACファイルを使用できるようになります。このとき、次のようなURLを使用します。`http://IP-of-ASG:8080/wpad.dat` このファイルを使用するには、プロキシを使用するブラウザの自動プロキシ構成設定にこのURLを入力します。

- DHCP経由で提供する:DHCPサーバがクライアントのIPアドレスと併せてPACファイルのURLを受け渡すようにすることもできます。これには、DHCPサーバの設定で【*HTTPプロキシ自動設定の有効化(Enable HTTP Proxy Auto Configuration)*】オプションを選択します(「*ネットワークサービス*」>>「DHCP」の章を参照してください)。これにより、ブラウザ

がPACファイルを自動的にフェッチし、それに従って設定を構成します。

> **注 -** DHCP経由での提供は、マイクロソフトのInternet Explorerのみで機能します。その他すべてのブラウザでは、PACファイルを手動で提供する必要があります。

その他の設定

Webフィルタポート(Web Filtering Port): ここで、Webフィルタがクライアントの要求に対して使用するポート番号を定義できます。デフォルトは`8080`です。

> **注 -** これが適用されるのは、プロキシを透過モードで操作していない場合のみです。

アクセスしたページのログ(Log Accessed Pages): 選択すると、要求のユーザ名とクライアントIPとともに、アクセスしたURLのログが記録されます。

ブロックされたページのログ(Log Blocked Pages): 選択すると、要求のユーザ名とクライアントIPとともに、ブロックされたURLのログが記録されます。

> **注 -** ログオプションは、除外(「*除外*」の項を参照)またはプロファイルのフィルタアクション(「*Webセキュリティ*」>>「*Webフィルタプロファイル*」>>「*フィルタアクション*」を参照)を利用して個別に設定することもできます。

スキャン不可能なファイルと暗号化されたファイルをブロック(Block Unscannable and Encrypted Files): スキャンできないファイルをブロックするには、このオプションを選択します。スキャンできない理由はいくつかありますが、ファイルが暗号化されているか、破損している可能性があります。

MIMEブロッキングでHTTP本文を検査(MIME Blocking Inspects HTTP Body): HTTPヘッダのみならず、HTTPボディも、ブロックされたMIMEタイプに対してチェックされます。この機能をオンにすると、パフォーマンスが低下する可能性があります。

許可されるターゲットサービス(Allowed Target Services):【*許可されるターゲットサービス(Allowed Target Services)*】ボックスでは、Webフィルタのアクセスが許可されるターゲットサービスを選択できます。デフォルト設定は、*HTTP*(ポート`80`)、*HTTPS*(ポート`443`)、*FTP*(ポート`21`)、*LDAP*(ポート`389`)、*LDAP-SSL*(ポート`636`)、*Webフィルタ*(ポート`8080`)、*Astaro Spam Release*(ポート`3840`~`4840`)、および*Astaro WebAdmin*(ポート`4444`)などのターゲットサービス(ポート)で構成されています。これらは、通常は安全に接続でき、ブラウザで一般に使用されています。

デフォルト文字セット(Default Charset): このオプションは、【*ダウンロードマネージャ(Download Manager)*】ウィンドウでプロキシがファイル名をどのように表示するかに影響を与えます。外国語の文字セットでエンコードされているURL(およびURLで参照されるファイル名)は、サーバが別の文字セットを送信する場合を除き、ここで指定されている文字セットからUTF-8に変換されます。ダブルバイト文字セットを使用する国または地域では、このオプションを当該国または地域の「ネイティブ」文字セットに設定する必要があります。

ドメインの検索(Search Domain): ここで、最初のDNSルックアップで結果が返されなかった("NXDOMAIN")場合に検索される追加のドメインを追加することができます。最初のDNSルックアップの次に、2番目のDNS要求が開始され、ここで指定したドメインをオリジナルのホスト名に追加します。例:ユーザが「`http://wiki`, meaning to address *wiki.intranet.example.com*」と入力します。ただし、URLは、【*ドメイン検索(Search Domain)*】フィールドに「`intranet.example.com`」と入力していなければ解決できません。

認証タイムアウト(Authentication Timeout): このオプションを使用すると、透過的なユーザ認証機能を使用しているときにユーザ認証の試行を行う間隔を秒単位で設定できます。

認証レルム(Authentication Realm): 認証レルムとは、プロキシが*基本ユーザ認証*モードで機能しているときに、ブラウザが認証要求とともに表示する送信元の名前です。認証レルムは、RFC 2617に基づいて保護スペースを定義します。ここでは任意の文字列を指定できます。

HTTP/S親プロキシルーティング(HTTP/S Parent Proxy Routing)

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国で必要とされます。1つ以上の親プロキシの使用がセキュリティポリシで求められている場合、ここで親プロキシを追加または選択できます。

ボックスが空の場合、まず、親プロキシの定義を作成してください。以下の手順に従ってください。

1. **ボックスヘッダの「+」アイコンをクリックします。**
   【*親プロキシの追加(Add Parent Proxy)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): この親プロキシを説明する名前を入力してください。

   コメント(Comment)(オプション):説明などの情報を追加します。

   これらのホストにプロキシを使用(Use Proxy for These Hosts): 親プロキシを使用するホストをこのボックスに追加します(例:`*.wikipedia.org`)。ここではパターンマッチを使用できます。ただし、正規表現は使用できません。ボックスを空にすると、【*保存(Save)*】をクリックするとアスタリスク(*)が自動的に追加され、すべてのホストに該当し

ます。従って、このようなプロキシ定義は、一致するプロキシが存在しない場合のフォールバックプロキシとみなされます。

親プロキシ(Parent Proxy): 親プロキシのネットワーク定義を選択または追加します。

ポート(Port): 親プロキシ接続のデフォルトポートは8080です。親プロキシで別のポートを使用する場合、ここで変更できます。

プロキシは認証が必要(Proxy Requires Authentication): 親プロキシが認証を必要とする場合は、チェックボックスにチェックを入れ、表示されるテキストボックスにユーザ名とパスワードを入力します。

3. ***【保存(Save)】*をクリックします。**
   新しい親プロキシが*【親プロキシ(Parent Proxies)】*ボックスに表示されます。

これで、このプロキシをフィルタアクションで使用することも、グローバルに使用することもできます。親プロキシ定義を編集または削除するには、*【Webフィルタプロファイル(Web Filtering Profiles)】>>【親プロキシ(Parent Proxies)】*ページに進みます。

各プロキシの前にあるチェックボックスにチェックを入れて、親プロキシの使用を有効化します。複数のプロキシを選択した場合、青い矢印を使用してプロキシを並べ替えることができます。選択した親プロキシは、最初のプロキシが一致するまで、所定の順序で適用されます。処理順序は位置番号によって決まるため、位置番号によってプロキシの順序を変更すると、処理順序も変わります。

親プロキシの使用は、プロファイルベースにすることもできます(詳しくは、*「Webフィルタプロファイル」>>「フィルタアクション」*の章を参照してください)。

親プロキシおよびWebサイトの分類(Parent Proxies and Website Categorization)

親プロキシ経由でデータベース更新の取得や分類ルックアップを行いたい場合は、この親プロキシに対して以下のホストを指定する必要があります。

- `list.smartfilter.com`(ローカル分類データベースの場合)
- `cffs*.astaro.com`(TCP分類の場合)

1つの親プロキシがすべてのホストに一致するように設定する場合(*)、これらのホストを指定する必要はありません。特定のホストに対して異なる親プロキシを定義し、最後の親プロキシがすべてのホストに一致するように(*)設定することもできます。この場合、このトラフィックのみが最後の親プロキシ経由でルーティングされ、他のすべての親プロキシは一致しません。

HTTPキャッシング(HTTP Caching)

キャッシングを有効化(Enable Caching): このオプションが有効になっている場合、Webフィルタはオンディスクオブジェクトキャッシュを保持して、アクセス頻度が高いWebページへの要求を高速化します。

SSLコンテンツのキャッシュ(Cache SSL Content): このオプションを有効にすると、SSL暗号化されたデータは、非暗号化形式でもディスクに保存されます。

Cookieを含むコンテンツをキャッシュ(Cache Content that Contains Cookies): Cookieは、一般に認証目的で使用されます。このオプションを有効にすると、Cookieが含まれるHTTP応答もキャッシュされます。複数のユーザが同じページを要求している場合、あるユーザのCookieが含まれるキャッシュページが他のユーザに提供される可能性があるため、この設定は重大です。

> **重要 -** SSLまたはCookieコンテンツ(あるいはその両方)をキャッシュすると、SuperAdmin権限を持つすべてのユーザがコンテンツを閲覧できるため、セキュリティ上の重要な問題です。

キャッシュのクリア(Clear Cache):【*キャッシュのクリア(Clear Cache)*】をクリックすると、キャッシュされたすべてのページを削除できます。

MAC OS Xシングルサインオン(MAC OS X Single Sign-On)

認証方式として*Apple OpenDirectory SSO*を使用している場合、認証が適切に機能するためには、MAC OS XシングルサインオンKerberos鍵ファイルをアップロードする必要があります。この鍵ファイルを生成し、【*鍵ファイルのアップロード(Upload Keyfile)*】をクリックしてアップロードします。鍵ファイルの生成方法について詳しくは、Kerberosのマニュアルを参照してください。

9.1.7HTTPS CA

【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*HTTPS CA(HTTPS CAs)*】タブでは、HTTPS接続の署名および検証CA(認証局)を管理できます。

署名CA(Signing CA)

このエリアでは、署名CA証明書のアップロード、署名CA証明書の再生成、または既存の署名CA証明書のダウンロードが可能です。デフォルトで署名CA証明書は、セットアップ中に提供された情報に基づいて作成されます。つまり、セットアップ後に何らかの変更が行われた場合を除き、【*マネジメント(Management)*】>>【*システム設定(System Settings)*】>>【*組織(Organizational)*】タブの情報と一致しています。

新しい署名CA証明書をアップロードするには、次の手順に従ってください。

1. ***【アップロード(Upload)】ボタンをクリックします。***
   *【PKCS#12証明書ファイルのアップロード(Upload PKCS#12 Certificate File)】*ダイアログボックスが開きます。

2. **アップロードする証明書までブラウズします。**
   *【ファイル(File)】*ボックスの横にあるフォルダアイコンをクリックし、*【ファイルのアップロード(Upload File)】*ダイアログボックスが開いたら*【参照(Browse)】*をクリックしてアップロードする証明書を選択し、*【保存(Save)】*をクリックします。

   パスワードで保護されているPKCS#12形式の証明書のみをアップロードできます。

3. **パスワードを入力します。**
   該当フィールドにパスワードをもう一度入力し、*【保存(Save)】*をクリックします。

   新しい署名CA証明書がインストールされます。

署名CA証明書を再生成するには、次の手順に従ってください。

1. ***【再生成(Regenerate)】ボタンをクリックします。***
   *【新規署名CAの作成(Create New Signing CA)】*ダイアログボックスが開きます。

2. **情報を変更します。**
   必要に応じて所定の情報を変更し、*【保存(Save)】*をクリックします。

   新しい署名CA証明書が生成されます。*これに基づき、【署名CA(Signing CA)】*エリア内の署名CA情報が変化します。

署名CA証明書をダウンロードするには、次の手順に従ってください。

1. ***【ダウンロード(Download)】ボタンをクリックします。***
   *【証明書ファイルのダウンロード(Download Certificate File)】*ダイアログボックスが開きます。

2. **ダウンロードするファイル形式を選択します。**
   2種類の形式から選択できます。

   - **PKCS#12**: この形式は暗号化されるため、エクスポートパスワードを入力してください。
   - **PEM**: 暗号化されない形式です。

3. ***【保存(Save)】をクリックします。***
   ファイルが保存されます。

カスタムCAで署名された証明書を内部Webサーバに対して使用する場合、信頼される認証局としてこのCA証明書をWebAdminにアップロードすることをお勧めします。これを行わないと、Webフィルタが、信頼できないサーバ証明書が検知されたというエラーメッセージをユーザに表

示します。
クライアントPCへのプロキシCA証明書の提供を円滑化するために、ユーザは自分でhttp://passthrough.fw-notify.net/cacert.pemから証明書をダウンロードし、ブラウザにインストールすることができます。Webサイト要求はプロキシで直接受信され、処理されます。そのため、まず【*Webセキュリティ(Web Security)*】>>【*グローバル(Global)*】タブでWebフィルタを有効にする必要があります。

注 - プロキシのオペレーションモードが*透過モード*ではない場合、ユーザのブラウザでプロキシを有効にする必要があります。有効にしないと、証明書ダウンロード用のリンクがアクセス不可になります。

あるいは、ユーザポータルが有効であれば、ユーザはプロキシCA証明書をユーザポータルの【*HTTPSプロキシ(HTTPS Proxy)*】タブからダウンロードできます。

HTTPSでの問題を回避する

HTTPSの使用中、Windows UpdateやWindows DefenderなどのWindowsシステムプログラムは接続を確立できません。これは、これらのプログラムがシステムユーザ権限で実行されるためです。このユーザはデフォルトで、プロキシCAを信頼しないことになっています。そのため、システムユーザ用にHTTPSプロキシCA証明書をインポートする必要があります。以下の手順に従ってください。

1. **Windowsで、*Microsoft管理コンソール*(mmc)を開きます。**
2. **【*ファイル*】メニューをクリックし、【*スナップインの追加と削除*】をクリックします。**
   【*スナップインの追加と削除*】ダイアログウィンドウが開きます。
3. **ウィンドウの一番下にある【*追加*】をクリックします。**
   【*スタンドアロン スナップインの追加*】ダイアログウィンドウが開きます。
4. **リストから【*証明書*】を選択し、【*追加*】をクリックします。**
   ウィザードが表示されます。
5. **【*コンピュータ アカウント*】を選択し、【*次へ*】をクリックします。**
6. **【*ローカル コンピュータ*】が選択されていることを確認し、【*完了*】>【*閉じる*】をクリックします。**
   最初のダイアログウィンドウに【*証明書(ローカル コンピュータ)*】が追加されています。
7. **【*OK*】をクリックします。**
   ダイアログウィンドウが閉じて、コンソールルートに【*証明書(ローカル コンピュータ)*】が追加されています。

8. **左側の【*コンソール ルート*】ウィンドウで【*証明書*】>>【*信頼されたルート証明機関*】を開き、【*証明書*】を右クリックして、コンテキストメニューの【*すべてのタスク*】>>【*インポート*】を選択します。**
   インポートダイアログウィザードが開きます。

9. **【*次へ(Next)*】をクリックします。**
   次のウィザードステップが表示されます。

10. **以前にダウンロードしたHTTPSプロキシCA証明書までブラウズし、【*開く*】>【*次へ*】をクリックします。**
    次のウィザードステップが表示されます。

11. **【*証明書をすべて次のストアに配置する*】が選択されていることを確認し、【*次へ*】>【*閉じる*】をクリックします。**
    インポートの成功がウィザードから報告されます。

12. **ウィザードのメッセージを確認します。**
    信頼される証明書の中に、プロキシCA証明書が表示されるようになりました。

13. **変更を保存します。**
    【*ファイル*】メニューをクリックし、【*保存*】をクリックして、コンソールルートでの変更を保存します。

インポート後、CAはシステム全体で受け入れられるようになり、HTTPプロキシに起因する接続問題は発生しなくなります。

検証CA(Verification CAs)

このエリアでは検証CAを管理できます。検証CAとは、最初に信頼する認証局です。つまり、これらのCAによって署名された有効な証明書を提示するWebサイトは、HTTPプロキシによって信頼できると見なされます。

ローカル検証CA(Local Verification CAs): 下のCAリストに追加して検証CAをアップロードできます。次の手順で実行します。

1. **【*ローカルCAのアップロード(Upload Local CA)*】フィールドの横のフォルダアイコンをクリックします。**
   【*ファイルのアップロード(Upload File)*】ダイアログボックスが開きます。

2. **アップロードする証明書を選択します。**
   【*参照(Browse)*】をクリックして、アップロードするCA証明書を選択します。

3. **証明書をアップロードします。**
【*アップロード開始(Start Upload)*】をクリックして、選択したCA証明書をアップロードします。

   証明書はインストールされ、【*ローカル検証CA(Local Verification CAs)*】エリアに表示されます。

グローバル検証CA(Global Verification CAs): ここに表示される検証CAのリストは、Mozilla Firefoxにあらかじめインストールされた検証CAと同じです。ただし、リストに含まれるいずれか(あるいは全部)の検証CAを「信頼できない」場合は、これらを無効にすることができます。CAの証明書を無効にするには、ステータスアイコンをクリックします。ステータスアイコンが赤色になり、HTTPSプロキシはこのCAに署名されたWebサイトを受け入れなくなります。

ヒント - CAのフィンガープリントを表示するには、青色の情報アイコンをクリックしてください。

CAが不明または無効である場合、HTTPSプロキシはクライアントに対して「ブロックされたコンテンツ」のエラーページを表示します。ただし、このようなページに対して除外を作成することができます。これには、Webフィルタのエラーページで【*除外の作成(Create Exception)*】リンクを使用するか、【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*除外(Exceptions)*】タブを使用します。

注 - Webフィルタのエラーページで【*除外の作成(Create Exception)*】リンクをクリックすると、ログインダイアログウィンドウが表示されます。admin権限のあるユーザのみが除外を作成できます。

9.2Webフィルタプロファイル

Astaro Security Gateway には、どのネットワークに対して何のWebコンテンツを利用可能にするかをコントロールするために設計、最適化されたWebフィルタが用意されています。これにより、好ましくないと考えるコンテンツを利用者が閲覧することを予防できます。Webフィルタを設定し、選択したネットワークに対してグローバルに適用することができます。あるいは、ネットワークのセグメント別に各種セキュリティポリシを適用するために個々のWebフィルタプロファイルを作成することができます。これにより、ユーザ認証方式が異なる場合でも、組織内の各部門に適した別々のコンテンツフィルタリングポリシを定義することができます。

クロスリファレンス - Webフィルタプロファイルの設定方法に関する詳しい説明は、Astaroナレッジベースを確認してください(*「ASGバージョン7」>>「Webセキュリティ」*の順にアクセスします)。

この章では、フィルタアクションの追加方法と、Webフィルタプロファイルフレームワークでフィルタアクションを使用する方法について説明します。Astaro Security Gateway.【*Webフィルタプロファイル(Web Filtering Profiles)*】タブの設定は、後方から前方に向かって進めることをお勧めします。つまり、フィルタアクションの指定から開始します。これらは、フィルタ割り当てで特定のユーザまたはユーザグループに割り当てます。次に、実際のWebフィルタプロファイルの設定に続きます。

9.2.1概要

注 - Webフィルタプロファイルを設定するためには、Webフィルタを有効にする必要があります。

このフローチャートは、フィルタアクション、フィルタ割り当て、Webフィルタプロファイルの間でどのようなやり取りがあるのかを示します。HTTPリクエストを受け取ると、Webフィルタはまず、どのWebフィルタプロファイルを適用すべきか判断します。これは、リクエストの送信元IPアドレスに完全に依存します。リクエストの送信元IPと一致する最初のプロファイルが使用されます。他のすべてのWebフィルタプロファイルは無視されます。

内部では、すべてのプロファイルが1つのファイルに保存され、デフォルトプロファイルはリストの一番下に配置されます。他のHTTPプロファイルが設定されていない初期段階には、デフォルトプロファイルが唯一のエントリとなります。個々のWebフィルタプロファイルを追加して、【*位置(Position)*】ドロップダウンリストでプロファイルをソートするようになると、デフォルトプロファイルはリストの一番下に留まり、常に一番最後に適用されるようになります。

ただし、デフォルトプロファイルは、【*Webセキュリティ(Web Security)*】>>【*Webフィルタプロファイル(Web Filtering Profiles)*】タブで明示的に設定するプロファイルではありません。【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】タブでHTTPプロキシをグローバルに設定すると自動的に作成されます。【*許可ネットワーク(Allowed Networks)*】は、Webフィルタプロファイルの*送信元ネットワーク*に対応する【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*グローバル(Global)*】タブで設定します【*ユーザ/グループ(Users/Groups)*】ボックスの設定(オペレーションモード【*基本ユーザ認証(Basic User Authentication)*】を選択すると【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*グローバル(Global)*】タブに表示される)は、デフォルトのフィルタ割り当てとなります。また、【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*URLフィルタリング(URL*

Filtering)】タブの設定は、フィルタアクションに対応します。最後に、デフォルトプロファイルでも一致しなかった場合、HTTP要求はブロックされます。

続いて、このWebフィルタプロファイルにどのフィルタ割り当てが関連付けられているのかをチェックします。フィルタ割り当てが一致しない場合、フォールバックアクションが要求に適用されます。フォールバックアクションとは、御社のセキュリティポリシを反映させるための特別なフィルタアクションです。厳格なセキュリティポリシを遵守する必要がある場合、例外なくすべてのWebトラフィックをブロックするフィルタアクションを作成することができます。

同じネットワークセグメント内の複数のユーザに対して、異なるレベルの防御を提供するには、異なるフィルタ割り当てを関連付けて1つのWebフィルタプロファイルを設定するだけです。特定のユーザに何が許可されるのかは、選択したフィルタ割り当ての順番に応じて決まります。このため、送信元ネットワークがまったく同じである2つのプロファイルを設定しても、2つ目のプロファイルはまったく使用されないため、意味がありません。

9.2.2 プロキシプロファイル

プロキシプロファイルを使用すると、複数のコンテンツフィルタリングポリシを作成し、ネットワーク内のさまざまなアドレスに別々のポリシを適用することができます。これにより、組織内のさまざまな部門に対して別々のポリシを定義できます。さらに、各プロキシプロファイルには独自のユーザ認証方式を設定できます。

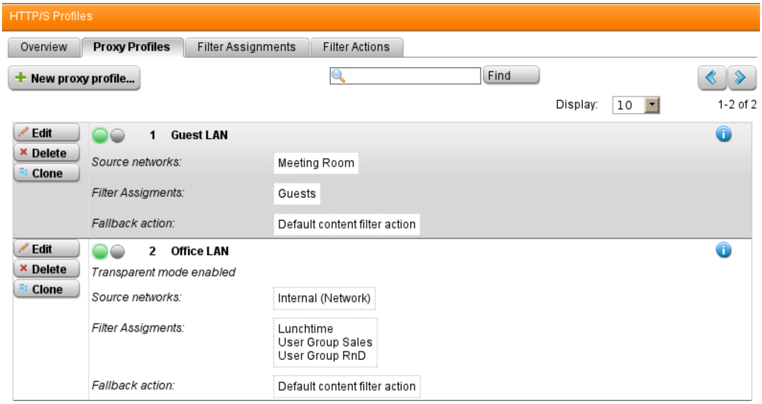


図83 Webフィルタプロファイル: プロファイルのリスト

プロキシプロファイルを作成するには、次の手順に従います。

1. ***【新規プロキシプロファイル(New Proxy Profile)】をクリックします。***
   【*プロキシプロファイルの作成*(*Create Proxy Profile*)】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): このプロファイルを説明する名前を入力してください。

   位置(Position): プロキシプロファイルの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。プロキシプロファイルは昇順に照合されます。あるプロキシプロファイルが一致すると、それ以降、それより大きい番号のプロキシプロファイルは評価されません。より詳細なプロファイルをリストの上部に配置することで、最も限定的でないプロファイルが最後に照合されるようになります。

   送信元ネットワーク(Source Networks): このプロキシプロファイルを使用するネットワークを選択します(これは必須フィールドです)。

   > **警告 -** ここでは、他のプロキシプロファイルで使用されている送信元ネットワークを選択しないでください。そのような送信元ネットワークを選択すると、コンテンツフィルタのアクションとユーザ/グループのマッピングに不整合が生じ、特定のネットワークセグメントに属するユーザが、本来アクセスすべきではないWebサイトを閲覧できるようになる可能性があります。

   フィルタ割り当て(Filter Assignments): フィルタ割り当てを選択します。フィルタ割り当てとは1セットのWebセキュリティ構成設定であり、これを使用すると、さまざまなユーザ/グループにさまざまなレベルの保護をさまざまなタイミングで割り当てることができます(詳しくは、「*Webセキュリティ*」>>「*Webフィルタプロファイル*」>>「*フィルタ割り当て*」を参照してください)。複数のフィルタ割り当てを選択することができます。さらに、どのフィルタ割り当てを最初に適用するのかを指定することができます。これは、同じユーザまたはユーザグループに対して、さまざまなフィルタ割り当てをさまざまなタイミングで適用したい場合に便利です。一般に、より詳細な割り当てをリストの上部に配置することで、最も限定的でない割り当てが最後に照合されるようになります。これには、2つ以上のフィルタを選択すると表示される青い矢印を使用します。

   > **注 -** Webフィルタが【*基本ユーザ認証(Basic User Authentication)*】、【*Active Directory SSO*】、または【*eDirectory SSO*】モードで実行されている場合は、【*デフォルトフィルタ割り当て(Default Filter Assignment)*】を選択することもできます。この割当では、【*Webフィルタリング(Web Filtering)*】>>【*グローバル(Global)*】タブで設定したユーザ/グループに【*デフォルトフィルタアクション(Default Filter Action)*】が割り当てられています。オペレーションモードを【*標準(Standard)*】または【*透過(Transparent)*】に設定した場合でも、ユーザやグループが選択されたフィルタ割り当てを使用することができ

ますが、この場合、このプロキシプロファイルの使用時に、当該のユーザやグループは無視され、フィルタ割り当てに指定された期間定義のみが考慮されます。

フォールバックアクション(Fallback Action): フォールバックアクションとは、会社のセキュリティポリシを反映するための特別なフィルタアクションであり、選択されたフィルタ割り当てがいずれも一致しない場合に、要求に適用されます。たとえば、厳格なセキュリティポリシを遵守する必要がある場合、例外なくすべてのWebトラフィックをブロックする特別なフィルタアクションをフォールバックとして作成することができます。また、ここで選択できる【*デフォルトフィルタアクション(Default Filter Action)*】は、【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*URLフィルタリング(URL Filtering)*】タブでの設定に対応しています。

オペレーションモード(Operation Mode): 各プロキシプロファイルに対し、複数のユーザ認証方式から選択することができます。異なるプロキシプロファイルに異なる認証方式を持たせることができますが、1つのプロキシプロファイルには1つの認証方式しか使用できません。【*Webフィルタリング(Web Filtering)*】>>【*グローバル(Global)*】タブで設定したオペレーションモード以外のオペレーションモードを選択することもできます。ただし、その認証が期待どおりに機能するのは、ここで選択した認証モードがすべてのフィルタ割り当てで使用されるすべてのユーザおよびグループオブジェクトの認証モードと一致している場合に限られます。次のオペレーションモードを使用できます。

- **標準(Standard)**: 標準モードでは、Webフィルタはデフォルトでクライアント要求をポート8080でリスンし、【*許可ネットワーク(Allowed Networks)*】ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。
- **Active Directory SSO**:【*定義およびユーザ(Definitions & Users)*】>>【*認証サーバ(Authentication Servers)*】>>【*サーバ(Servers)*】タブで*Active Directoryシングルサインオン*(SSO)を設定した場合、これを選択します。これにより、NTLMユーザ認証が認証クライアントで使用されます。動作が保証されるのはInternet Explorerのみです。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。
- **Apple OpenDirectory SSO**:【*ユーザおよび定義(Definitions & Users)*】>>【*認証サーバ(Authentication Servers)*】>>【*サーバ(Servers)*】タブで*LDAP*を設定しており、Apple OpenDirectoryを使用している場合、これを選択します。さらに、プロキシが正しく機能するようにするためには、【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*詳

細(Advanced)】タブで、MAC OS XシングルサインオンKerberos鍵ファイルをアップロードする必要があります。Webフィルタをこのモードで使用する場合、クライアントはブラウザ設定でWebフィルタを指定しておく必要があります。Safariブラウザ
はSSOをサポートしていません。

- **基本ユーザ認証(Basic User Authentication)**: このモードでは、各クライアントはプロキシを使用する前にこのプロキシに対して自己認証する必要があります。サポートされる認証方式について詳しくは、「*定義およびユーザ*」>>「*認証*」を参照してください。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。
- **eDirectory SSO**:【*定義およびユーザ(Definitions & Users)*】>>【*認証サーバ(Authentication Servers)*】>>【*サーバ(Servers)*】タブで*eDirectory*を設定した場合、これを選択します。このモードで使用する場合、クライアントはブラウザの設定でWebフィルタにHTTPプロキシを指定していることが必要です。
- **透過(Transparent)**: 透過モードでは、ポート`80`(SSLを使用している場合はポート`443`)でクライアントブラウザアプリケーションが行うすべての接続はインターセプトされ、クライアント側の設定なしでプロキシにリダイレクトされます。クライアントがプロキシサーバを意識することは全くありません。このモードの利点は、追加の管理やクライアント側での設定が不要であることで、短所は、処理できるのがHTTP(ポート80)要求のみであることです。そのため、*透過*モードを選択すると、クライアントのプロキシ設定は無効になります。

  フル透過モード(Full Transparent Mode)(オプション):クライアントの送信元IPをゲートウェイのIPに置き換えず、そのまま維持する場合は、【*完全透過モード(Full Transparent Mode)*】チェックボックスにチェックを入れます。これは、クライアントがパブリックIPアドレスを使用しており、プロキシによって隠すべきではない場合に便利です。

注 - 透過モードでは、プロキシはHTTP要求からNTLM認証ヘッダを削除します。さらに、プロキシはこのモードではFTP要求を処理できません。クライアントがこのようなサービスにアクセスする必要がある場合は、ファイアウォールでポート(`21`)を開く必要があります。一部のWebサーバは、ポート80以外のポート経由でストリーミング動画や音声などのデータを送信します。これらの要求は、プロキシが透過モードで機能しているときは検知されません。このようなトラフィックにも対応したい場合には、他のモードを使用するか、これらを許可する明確なファイアウォールルールを入力する必要があります。

- **認証付き透過(Transparent with Authentication)**: このモードは、プロキシを透過的に機能させながら、ユーザに認証を強制する場合に使用します。ユーザがあるWebサイトを初めて開くと、認証ユーザポータルのようなWebページが表示され、ユーザはユーザ名とパスワードを入力する必要があります。このモードでは、クライアント側のブラウザ設定なしで、ユーザ名に基づく追跡、報告、およびサーフィンが可能になります。さらに、そのダイアログウィンドウに追加で免責条項を表示することができます。この場合、ユーザが先に進むためには、免責条項に同意する必要があります。免責条項について詳しくは、「*マネジメント*」>>「*カスタマイズ*」>>「*Webフィルタ*」の章を参照してください。

HTTPS(SSL)トラフィックのスキャン(Scan HTTPS(SSL)Traffic): HTTPトラフィックに加えHTTPSトラフィックもスキャンする場合は、このチェックボックスにチェックを入れます。

コメント(Comment)(オプション): 説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
新しいプロファイルが【*プロキシプロファイル(Proxy Profiles)*】リストに表示されます。

プロキシプロファイルを編集または削除するには、対応するボタンをクリックします。

9.2.3フィルタ割り当て

*【Webフィルタプロファイル(Web Filtering Profiles)】>>【フィルタ割り当て(Filter Assignment)】*タブでは、特定のユーザおよびユーザグループにフィルタアクションを割り当てることができます。フィルタアクションでは、ブロックすべきWebサイトやWebサイトカテゴリを定義することによって「何を」に焦点をあてますが、フィルタ割り当てでは、これらのアクションを特定のタイミングでユーザとユーザグループに割り当てることによって「誰」と「いつ」に焦点をあてます。

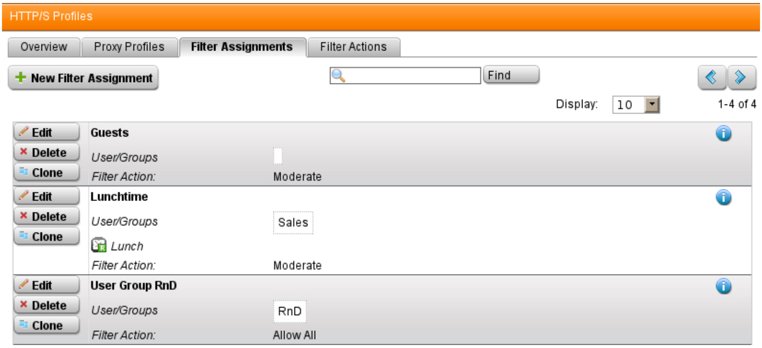


図84 Webフィルタプロファイル: フィルタ割り当てのリスト

注 -『*Webセキュリティ(Web Security)*』>>『*Webフィルタリング(Web Filtering)*』>>『*アンチウイルス/マルウェア(AntiVirus/Malware)*』タブで行った各種設定(アンチウイルススキャン、ファイル拡張子フィルタ、MIMEタイプフィルタ、コンテンツ削除)と『*URLフィルタリング(URL Filtering)*』タブで行った各種設定(カテゴリ、ブロックするURL)は、下の『*フィルタアクション(Filter Action)*』ドロップダウンリストで選択できる『*デフォルトフィルタアクション(Default Filter Action)*』として保存されます。

フィルタ割り当てを作成するには、次の手順に従います。

1. ***『新規フィルタ割り当て(New Filter Assignment)』をクリックします。***
   『*新規フィルタ割り当ての作成(Create New Filter Assignment)*』ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name): この割り当てを説明する名前を入力してください。

   ユーザ/グループ(Users/Groups): 特定のフィルタアクションを使用すべきユーザとグループを選択します。新しいフィルタ割り当ては、ここで選択したユーザおよびグループと同じ認証モードを使用するWebフィルタプロファイルのみに追加する必要があります。

   期間(Time Period): タイムイベントとは、ファイアウォールルールやフィルタプロファイルを特定の時間範囲に制限するために使用できる単一の(または繰り返される)時間帯(タイムスロット)です。詳細は、『*定義およびユーザ(Definitions & Users)*』>>『*期間定義(Time Period Definitions)*』を参照してください。

   フィルタアクション(Filter Action): 上で定義したユーザとユーザグループに割り当てるフィルタアクションを選択します。

   コメント(Comment)(オプション):説明などの情報を追加します。
3. ***『保存(Save)』をクリックします。***
   新しい割り当てが『*フィルタ割り当て(Filter Assignments)*』リストに表示されます。

フィルタ割り当てを編集または削除するには、対応するボタンをクリックします。

Webフィルタプロファイルの作成時に、各フィルタ割り当てを選択できます。

9.2.4フィルタアクション

『*Webフィルタプロファイル(Web Filtering Profiles)*』>>『*フィルタアクション(Filter Actions)*』タブでは、一連のWebセキュリティ構成設定を作成および編集できます。この設定を使用して、さまざまなタイプやレベルの保護をカスタマイズすることが可能です。フィルタアクションは、さまざまな

ユーザやユーザグループに割り当てることができ、Webアクセスをコントロールするための柔軟な手法となります。

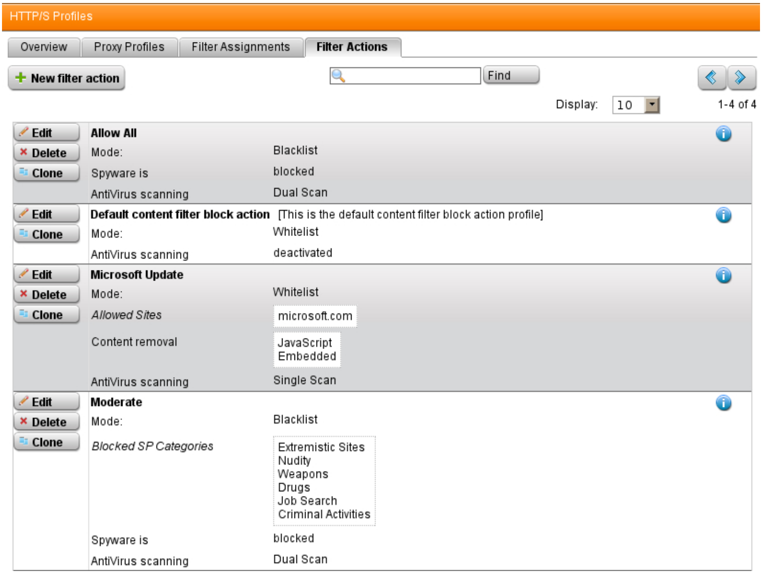


図85 Webフィルタプロファイル:フィルタアクションのリスト

フィルタアクションを作成するには、次の手順に従います。

1. ***【新規フィルタアクション(New Filter Action)】をクリックします。***
   *【新規フィルタアクションの作成(Create New Filter Action)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): このアクションを説明する名前を入力してください。

   モード(Mode): 選択したWebサイトをブロックするか許可するかを選択します。次のオプションを使用できます。

   - **デフォルトで許可(Allow By Default)**: このオプションを選択すると、選択したWebサイトはブロックされますが、他のすべてのWebサイトは許可されます。

   - **デフォルトでブロック(Block By Default)**: このオプションを選択すると、選択したWebサイトを除くすべてのWebサイトがブロックされます。

しきい値(Threshold): Webサイトは「*信頼される(Trusted)*」、「*中立(Neutral)*」、「*疑わしい(Suspicious)*」のいずれかに分類できます。未分類のWebサイトを「*未確認(Unverified)*」と呼びます。ネットワークからアクセスできるWebサイトがどのような評判を持つべきかを決定することができます。選択したしきい値を下回るWebサイトはブロックされます。

スパイウェア通信をブロック(Block Spyware Communication):このオプションを選択すると、サーバからクライアントへのトラフィックでスパイウェアを検出し、ブロックします。これにより、ネットワーク内のコンピュータが新しいスパイウェアに感染するのを防ぐことができます。さらに、この機能を有効にすると、すでにインストールされているスパイウェアアプリケーションについても検出し、トラフィックをブロックできます。この結果、スパイウェアが収集したユーザ情報がインターネットに送信されなくなります。このオプションは、モードを【*デフォルトでブロック(Block By Default)*】に変更すると使用できません。

これらのWebサイトカテゴリをブロック(Block these Website Categories):ブロックするWebサイトカテゴリを選択します。前述の【*モード(Mode)*】を【*デフォルトでブロック(Block By Default)*】に設定した場合、このオプションは【*これらのWebサイトカテゴリを許可(Allow these Website Categories)*】に変わります。

未分類サイトをブロック(Block Uncategorized Sites): このオプションを選択すると、未知のコンテンツを持つWebサイトをブラウザで開けなくなります。この機能は、好ましくないと思われるWebサイトが相応の分類をされていない場合のフォールバックセキュリティメカニズムと考えることができます。前述の【*モード(Mode)*】を【*デフォルトでブロック(Block By Default)*】に設定した場合、このオプションは【*未分類のサイトを許可(Allow Uncategorized Sites)*】に変わります。

これらのURL/サイトをブロック(Block these URLs/Sites): ブロックするサイトのURLを入力します。

常に許可するURL/サイト(Always Allow these URLs/Sites): 常に許可するサイトのURLを入力します。

SafeSearch: Google、Bing、Yahooの各検索エンジンに対してSafeSearchの使用を強制することができます。SafeSearchフィルタは、子供にふさわしくないコンテンツ(犯罪や不正)を検索結果から削除します。有効にすると、Webフィルタ経由でWebサーフィンをするユーザはフィルタをオフにできません。

ブロックするファイル拡張子(Blocked File Extensions):ファイル拡張子を指定すると、拡張子に基づいて特定タイプのファイルをブロックすることができます(実行可能バイナリなど)。ファイル拡張子を追加するには、【*ブロックするファイル拡張子(Blocked File*

Extensions)】ボックスの「+」アイコンをクリックし、ブロックしたい拡張子(exeなど)を入力します。区切り文字のドットは不要です。

ブロックするMIMEタイプ(Blocked MIME Types):ブロックするMIMEタイプを追加するには、【*ブロックするMIMEタイプ(Blocked MIME Types)*】ボックスの「+」アイコンをクリックし、MIMEタイプを入力します(image/gifなど)。

コンテンツ削除(Content Removal):これを選択すると、【*JavaScriptを削除(Remove JavaScript)*】オプションと【*埋め込みを削除(Remove Embedded)*】オプションが表示されます。これらのオプションを使用して、<SCRIPT>タグと<OBJECT>タグをHTMLページから削除するか否かを設定できます。【JavaScriptを削除(Remove JavaScript)】オプションを使用すると、HTMLページに埋め込まれた(またはHTMLページからインクルードされた)JavaScriptが無効になり、【埋め込みを削除(Remove Embedded)】を使用すると、受信側HTTP/SトラフィックからActiveX、Flash、Javaアプレットなどの動的コンテンツが除外されます。

アンチウイルススキャンを使用(Use AntiVirus Scanning): このオプションを選択すると、受信側Webトラフィックに悪質なコンテンツが含まれていないかスキャンが行われます。Astaro Security Gateway は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

最大スキャンサイズ(Max Scanning Size): アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

労働協議会のスタッフや会員など、アクティビティをロギングすべきではない人がいる場合には、次の2つのオプションが便利です。

- **アクセスしたページのログ(Log Accessed Pages)**: チェックを外すと、アクセスしたページがロギングやレポーティングから除外されます。
- **ブロックされたページのログ(Log Blocked Pages)**: チェックを外すと、ブロックされたページがロギングやレポーティングから除外されます。

親プロキシ(Parent Proxies): 1つ以上の親プロキシを使用することを決定できます。ボックスが空の場合、まず、【*親プロキシ(Parent Proxies)*】タブに親プロキシの定義を作成してください。親プロキシ定義の前にあるチェックボックスにチェックを入れると、使用が有効化されます。複数のプロキシがある場合、青い矢印をクリックして並べ替えることができます。選択した親プロキシは、最初のプロキシが一致するまで、所定の順序で適用されます。処理順序は位置番号によって決まるため、位置番号によってプロキシの順序を変更すると、処理順序も変わります。

3. **【*保存(Save)*】をクリックします。**
   新しいフィルタアクションが【*フィルタアクション(Filter Actions)*】リストに表示されます。

フィルタアクションを編集または削除するには、対応するボタンをクリックします。

フィルタ割り当てまたはWebフィルタプロファイルの作成時に、各フィルタアクションを選択できます。

> **注 -** ここでは、【*デフォルトのコンテンツフィルタブロックアクション(Default Content Filter Block Action)*】も参照できます。デフォルトでは、【*Webフィルタリング(Web Filtering)*】メニューの他のすべてのフィルタアクションや設定と一致しないHTTP/Sリクエストがすべてブロックされます。

9.2.5親プロキシ

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国で必要とされます。【*Webセキュリティ(Web Security)*】>>【*Webフィルタプロファイル(Web Filtering Profiles)*】>>【*親プロキシ(Parent Proxies)*】ページでは、親プロキシの使用を、プロファイルに基づくかグローバルに設定できます。親プロキシをプロファイルで使用するためには、常に、このページで(あるいは【*Webフィルタリング(Web Filtering)*】>>【*詳細(Advanced)*】ページで)最初に設定する必要があります。

> **注 -** 技術的な理由から、親プロキシを有効化した場合は、SSLスキャニングを有効化した状態での透過モードでのHTTPS要求はできません。

親プロキシを設定するには、次の手順に従います。

1. **【*新規親プロキシ(New Parent Proxy)*】をクリックします。**
   【*新規親プロキシ作成(Create New Parent Proxy)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): この親プロキシを説明する名前を入力してください。

   コメント(Comment)(オプション):説明などの情報を追加します。

   これらのホストにプロキシを使用(Use Proxy for These Hosts): 親プロキシを使用するホストをこのボックスに追加します(例:`*.wikipedia.org`)。ここではパターンマッチを使用できます。ただし、正規表現は使用できません。ボックスを空にすると、【*保存(Save)*】をクリックするとアスタリスク(*)が自動的に追加され、すべてのホストに該当します。従って、このようなプロキシ定義は、一致するプロキシが存在しない場合のフォールバックプロキシとみなされます。

   親プロキシ(Parent Proxy): 親プロキシのネットワーク定義を選択または追加します。

ポート(Port): 親プロキシ接続のデフォルトポートは8080です。親プロキシで別のポートを使用する場合、ここで変更できます。

プロキシは認証が必要(Proxy Requires Authentication): 親プロキシが認証を必要とする場合は、チェックボックスにチェックを入れ、表示されるテキストボックスにユーザ名とパスワードを入力します。

3. ***【保存(Save)】*をクリックします。**
新しい親プロキシが【*親プロキシ(Parent Proxies)*】リストに表示されます。

これで、このプロキシをフィルタアクションで使用することも、グローバルに使用することもできます。

親プロキシを編集または削除するには、対応するボタンをクリックします。

9.3アプリケーションコントロール

ASGのアプリケーションコントロール機能を使用すると、トラフィックの種類に基づいてネットワークトラフィックをシェーピングおよびブロックすることができます。ASGのWebフィルタ機能(「Webフィルタ」の章を参照)と違い、アプリケーションコントロール分類エンジンはネットワークトラフィックを、プロトコルやURLではなく、よりきめ細かい基準で識別することができます。これは、Webトラフィックに関して特に便利です。Webサイトへのトラフィックでは、通常、HTTP プロトコルをポート80で、あるいはHTTPS プロトコルをポート443で使用します。特定のWebサイト(facebook.comなど)へのトラフィックをブロックしたい場合、WebサイトのURL(Webフィルタ)に基づいてブロックすることができます。あるいは、ネットワークトラフィック分類を利用して、あらゆるURLから独立してfacebookトラフィックをブロックすることができます。

ASGの分類エンジンは、ネットワークトラフィックの分類にレイヤ7パケット検査を使用します。

アプリケーションコントロールは2つの方法で使用できます。最初のステップでは、【*ネットワークの可視性(Network Visibility)*】ページでアプリケーションコントロールを一般的に有効化する必要があります。これにより、アプリケーションがある程度「可視化」されます。これをこのまま(または、特定の時間だけ)残し、ユーザに使用されているアプリケーション(フローモニタ、ロギング、レポーティングなど)を確認することができます。2番目のステップでは、特定のアプリケーションをブロックし、他のアプリケーションは許可することができます。これには、【*アプリケーションコントロールルール(Application Control Rules)*】ページで作成するルールを使用します。さらに、トラフィックシェーピングを使用して、定義したアプリケーションのトラフィックに特権を与えることができます。この設定は、Astaroのサービス品質機能で行います。

9.3.1 ネットワークの可視性

*【Webセキュリティ(Web Security)】>>【アプリケーションコントロール(Application Control)】>>【ネットワークの可視性(Network Visibility)】*ページでは、アプリケーションコントロールを有効化または無効化できます。

アプリケーションコントロールを有効化すると、すべてのネットワークトラフィックが、その分類に応じて分類またはロギングされます。現在のネットワークトラフィックは、フローモニタに、タイプに関する詳細な情報と共に表示されます(「フローモニタ」の章を参照)。たとえば、HTTPトラフィックに関する情報は、おおもとのアプリケーション(「twitter」、「facebook」など)までドリルダウンされます。ロギングとレポーティングでは、ネットワークトラフィックとその分類に関する幅広い情報と、これらのアプリケーションを使用するクライアントとサーバの情報が表示されます。ロギングとレポーティングについて詳しくは、「*ロギングおよびレポーティング*」の章で、「*ログファイルの閲覧*」セクションを参照するか(ロギング)、「*ネットワーク使用状況*」>>「*帯域幅使用率*」セクションおよび「*Webセキュリティ*」>>「*アプリケーションコントロール*」セクションを参照してください(レポーティング)。

9.3.2 アプリケーションコントロールルール

*【Webセキュリティ(Web Security)】>>【アプリケーションコントロール(Application Control)】>>【アプリケーションコントロールルール(Application Control Rules)】*ページでは、ネットワークに対してトラフィックをブロックするか、または明示的に許可するアプリケーションを定義するネットワークトラフィック分類に基づいて、ルールを作成することができます。

デフォルトでは、アプリケーションコントロールを有効にするとすべてのネットワークトラフィックが許可されます。

アプリケーションコントロールルールの作成は、このページでもフローモニタでも可能です。フローモニタの方が使いやすいですが、ルールを作成できるのは、ネットワークで現在モニタリングされているトラフィックに対してのみです。

アプリケーションコントロールルールを作成するには、以下の手順に従います。

1. ***【アプリケーションコントロールルール(Application Control Rules)】*タブで、*【新規ルール(New Rule)】*をクリックします。**
   *【新規ルール作成(Create New Rule)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name)(オプション):ルールの名前を入力します。フィールドを空のままにすると、システムがルールの名前を生成します。

グループ(Group):【*グループ(Group)*】オプションを使用すると、アプリケーションコントロールルールを論理的にグループ化し、ルールセットを見やすくできます。グループ化は表示用のみで、ルールの一致には関係ありません。

位置(Position): 位置番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

アクション(Action): トラフィックをブロックするか許可するかを選択します。

コントロール基準(Control By): アプリケーションタイプに基づいてトラフィックをコントロールするか、分類に基づくダイナミックフィルタによってコントロールするかを選択します。

- **アプリケーション(Applications)**: トラフィックは、アプリケーションに基づいてコントロールされます。【*コントロール対象のアプリケーション(Control These Applications)*】ボックスでアプリケーションを1つ以上選択します。
- **ダイナミックフィルタ(Dynamic Filter)**: トラフィックは、分類に基づいてコントロールされます。【*コントロール対象の分類(アプリケーション)*】ボックスで分類を1つ以上選択します。

コントロール対象のアプリケーション/分類(Control These Applications/Categories): フォルダアイコンをクリックして、アプリケーション/分類を選択します。ダイアログウィンドウが開きます。これについては、次のセクションで詳しく説明します。

生産性(Productivity):*ダイナミックフィルタのみ*。選択した生産性スコアが反映されます。

リスク(Risk):*ダイナミックフィルタのみ*。選択したリスクスコアが反映されます。

注 - 一部のアプリケーションはブロックすることができません。これは、Astaro Security Gatewayの適切なオペレーションのために必要です。このようなアプリケーションは、【*アプリケーション選択(Select Application)*】ダイアログウィンドウのアプリケーションテーブルでチェックボックスがオフになっています。たとえば、*WebAdmin*、*Teredo*、*SixXs*(IPv6トラフィック用)、*Portal*(ユーザポータルのトラフィック用)などが該当します。ダイナミックフィルタを使用すると、これらのアプリケーションのブロックも自動的に制限されます。

対象(For): このルールによってネットワークトラフィックをコントロールするネットワークまたはホストを選択するか、このボックスに追加します。これは、送信元および宛先ホスト/ネットワークの両方に適用されます。

ログ(Log): このオプションはデフォルトでオンになっており、ルールと一致するトラフィックのロギングが有効になります。

コメント(Comment)(オプション): 説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**

   新しいルールが*【ルール(Rules)】*リストに表示されます。

4. **ルールを有効にします。**
   ルールを有効にするには、ステータスアイコンをクリックします。

【アプリケーションまたはカテゴリの選択(Select Application or Category)】ダイアログウィンドウ

アプリケーションコントロールルールを作成する際は、*【コントロール対象のアプリケーション/カテゴリを1つ以上選択(Select one or more Applications/Categories to control)】*というダイアログウィンドウからアプリケーションまたはアプリケーションカテゴリを選択する必要があります。

ダイアログウィンドウの下部に表示されるテーブルには、選択可能なアプリケーションまたは定義したカテゴリに属するアプリケーションが表示されます。デフォルトでは、すべてのアプリケーションが表示されます。

ダイアログウィンドウの上部には、テーブルに表示されるアプリケーション数を制限するための3つの設定オプションがあります。

- **Category(カテゴリ)**: アプリケーションはカテゴリ別にグループ分けされています。このリストには、利用可能なすべてのカテゴリが表示されます。デフォルトでは、すべてのカテゴリが選択されています。つまり、下部に表示されるテーブルには、利用可能なすべてのアプリケーションが表示されます。表示されるアプリケーションを特定のカテゴリに絞り込むには、クリックしてカテゴリリストを開き、1つ以上のカテゴリを選択します。

- **生産性(Productivity)**: アプリケーションは、生産性への影響(つまり生産性にこのアプリケーションが与える影響の度合い)によっても分類されています。例:一般的なビジネスソフトウェアのSalesforceのスコアは5です。つまり、これを使用することで生産性が向上します。一方、オンラインゲームのFarmvilleのスコアは1で、これを使用すると生産性が低下します。ネットワークサービスDNSのスコアは3で、生産性への影響は中立的です。

- **リスク(Risk)**: アプリケーションは、使用時のリスク(マルウェア、ウイルス感染、攻撃)によっても分類されています。数値が高いほど、リスクも高くなります。

ヒント - それぞれのアプリケーションには情報アイコンがあり、クリックすると各アプリケーションの説明が表示されます。テーブルヘッダの検索ボックスを使用して、テーブル内を検索することができます。

次に、*【新規ルール作成(Create New Rule)】*ダイアログウィンドウで選択したコントロールのタイプに応じて、以下を行います。

- ダイナミックフィルタでコントロールする場合：*【適用(Apply)】*をクリックして、選択したアプリケーションをルールに適用します。
- アプリケーションでコントロールする場合：テーブルで、アプリケーションの前のチェックボックスをクリックし、コントロール対象のアプリケーションを選択します。*【適用(Apply)】*をクリックして、選択したアプリケーションをルールに適用します。

*【適用(Apply)】*をクリックするとダイアログウィンドウが閉じ、アプリケーションルールの設定の編集を続けることができます。

9.3.3詳細

*【Webセキュリティ(Web Security)】>>【アプリケーションコントロール(Application Control)】>>【詳細(Advanced)】*ページでは、アプリケーションコントロールの詳細オプションを設定できます。

Astaro AppAccuracyプログラム

Astaro AppAccuracyプログラムに参加すると、ネットワークの可視性とアプリケーションコントロールの認識と分類の向上に貢献することができます。このシステムは、匿名アプリケーション指紋という形でデータを収集し、Astaroのリサーチチームへ送信します。ここでは、指紋を使用して、未分類のアプリケーションを識別し、ネットワーク可視性およびアプリケーションコントロールライブラリを改良および拡張します。

アプリケーションコントロールのスキップリスト

このボックスにリストされているホストとネットワークは、アプリケーションコントロールの監視対象とはならないため、アプリケーションコントロールで管理することも、サービス品質のアプリケーションセレクタで管理することもできません。これは、送信元および宛先ホスト/ネットワークの両方に適用されます。

9.4FTP

*【Webセキュリティ(Web Security)】>>【FTP】*タブでは、FTPプロキシを設定できます。*FTP(File Transfer Protocol)*は、インターネット上でのファイルのやり取りに幅広く使用されているプロトコルです。Astaro Security Gateway は、ネットワークを通過するすべてのFTPトラフィックの仲介役となるプロキシサービスを提供します。FTPプロキシには、FTPトラフィックのウイルススキャンや、FTPプロトコル経由で転送される特定のファイルタイプのブロックといった便利な機能が用意されています。

FTPプロキシは透過的に機能できます。つまり、ネットワーク内のすべてのFTPクライアントは、最終宛先ではなくプロキシへの接続を確立します。続いて、クライアントから見えない状態でプロキシが要求に代わって新しいネットワーク接続を開始します。このモードのメリットは、その他の管理やクライアント側の設定が必要ないということです。

9.4.1グローバル

*【Webセキュリティ(Web Security)】>>【FTP】>>【グローバル(Global)】*タブでは、FTPプロキシの基本設定を構成できます。

図86 FTPプロキシ(FTP Proxy):FTPプロキシを有効にする

FTPプロキシを設定するには、次の手順に従ってください。

1. ***【グローバル(Global)】*タブで、FTPプロキシを有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

ステータスアイコンがアンバー色になり、【*FTP設定(FTP Settings)*】エリアが編集可能になります。

2. **許可するネットワークを選択します。**
FTPプロキシの使用を許可するネットワークを選択します。

3. **オペレーションモードを選択します。**
FTPプロキシのオペレーションモードを選択します。次のモードを使用できます。

    - **透過(Transparent)**: プロキシは、クライアントの要求をターゲットサーバに転送し、コンテンツをスキャンします。クライアント側での設定は不要です。
    - **非透過(Non-Transparent)**: このモードを使用する場合、FTPクライアントを設定する必要があります。ゲートウェイのIPアドレスとポート`2121`を使用します。
    - **両方(Both)**: このモードを使用すると、一部のクライアントには透過モードを、他のクライアントには非透過モードを使用することができます。非透過モードで機能させるFTPクライアントを、ゲートウェイのIPアドレスとポート`2121`でプロキシを使用するように設定します。

4. **【*適用(Apply)*】をクリックします。**
設定が保存されます。

注 - FTPプロキシは、Active Directory認証を使用するFTPサーバとは通信できません。FTPクライアントがこのようなFTPサーバに接続できるようにするには、このサーバをFTPプロキシのスキップリストに追加します。スキップリストの設定は、【*Webセキュリティ(Web Security)*】>>【*FTP*】>>【*詳細(Advanced)*】タブで行います。

9.4.2アンチウイルス

【*Webセキュリティ(Web Security)*】>>【*FTP*】>>【*アンチウイルス(AntiVirus)*】タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを伝送するFTPトラフィックに対して講じることができるあらゆる対策が含まれています。

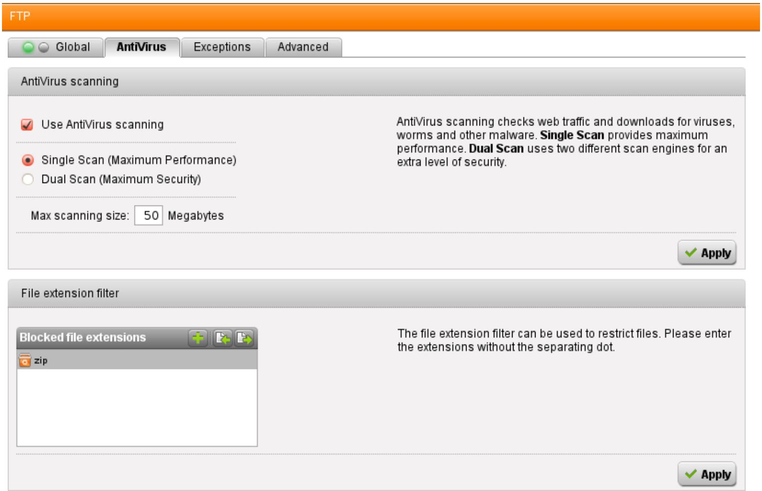


図87 FTPプロキシ(FTP Proxy):アンチウイルス設定の構成

アンチウイルススキャンを使用(Use AntiVirus Scanning): このオプションを選択すると、FTPトラフィック全体がスキャンされます。Astaro Security Gateway は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン(Single Scan)**: デフォルトの設定で、最高のパフォーマンスを提供します。
- **デュアルスキャン(Dual Scan)**: すべてのFTPトラフィックに対し、異なるウイルススキャナを使用してスキャンを2回行うことにより、検知率を最大限に高めます。

最大スキャンサイズ(Max Scanning Size): アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。設定を保存するには【*適用(Apply)*】をクリックします。

注 - 暗号化された`zip`アーカイブは、悪意あるコンテンツについてスキャンすることはできず、ウイルススキャナを通過します。暗号化された`zip`ファイルに含まれるマルウェアからネットワークを保護するために、`zip`ファイル拡張子をすべてブロックすることを検討してください。

ファイル拡張子フィルタ(File Extension Filter)

この機能では、ファイルの拡張子(実行可能バイナリなど)に基づいて、【*ブロックするファイル拡張子(Blocked File Extensions)*】ボックスにファイル拡張子がリストされているタイプのファイルを伝送するFTP転送をWebトラフィックからフィルタします。ファイル拡張子を追加したり、ブロック対象から外すファイル拡張子を削除したりすることができます。ファイル拡張子を追加するには、【*ブロッ*

クするファイル拡張子(Blocked File Extensions)】ボックスの「+」アイコンをクリックし、ブロックしたいファイル拡張子(exeなど)を入力します。区切り文字のドットは不要です。設定を保存するには【*適用(Apply)*】をクリックします。

9.4.3除外

【*FTP*】>>【*除外(Exceptions)*】タブでは、FTPプロキシの提供する選択可能なセキュリティオプションから除外するホワイトリストのホスト/ネットワークを定義することができます。

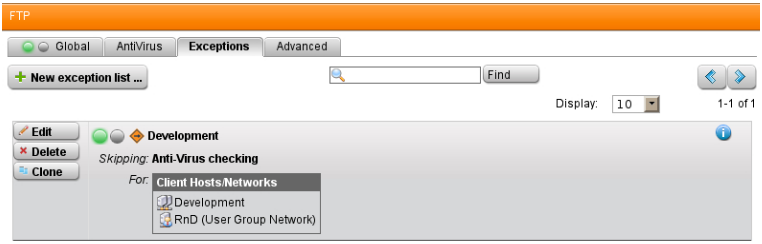


図88 FTPプロキシ(FTP Proxy):除外リスト

除外ルールを作成するには、次の手順に従います。

1. ***【除外(Exception)】タブで、【新規除外リスト(New Exception List)】をクリックします。***
   【*除外リストを作成(Create Exception List)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name):この除外を説明する名前を入力します。

   スキップするチェック(Skip These Checks):スキップするセキュリティチェックを選択します。

   - **アンチウイルスチェック(AntiVirus Checking)**:選択すると、ウイルスやトロイの木馬などの好ましくないコンテンツがトラフィックに含まれていないかチェックするウイルススキャンが無効になります。
   - **拡張子ブロック(Extension Blocking)**:選択すると、ファイル拡張子フィルタが無効になります。このフィルタは、ファイル拡張子に基づいてファイル転送をブロックするために使用します。
   - **許可サーバ(Allowed Servers)**:選択すると、【*詳細(Advanced)*】タブで設定できる、許可サーバのチェックが無効になります。

スキップするクライアントホスト/ネットワーク(For These Client Hosts/Networks): このオプションを選択すると、【*クライアントホスト/ネットワーク(Client Hosts/Networks)*】ボックスが開きます。この除外ルールのセキュリティチェックから除外するクライアントホスト/ネットワークを選択します。

サーバホスト/ネットワークで除外(For These Server Hosts/Networks): このオプションを選択すると、【*サーバホスト/ネットワーク(Server Hosts/Networks)*】ボックスが開きます。この除外ルールのセキュリティチェックから除外するサーバを選択します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
新しい除外が【*除外(Exceptions)*】リストに表示されます。

例外を編集または削除するには、対応するボタンをクリックします。

9.4.4詳細

【*FTP*】>>【*詳細(Advanced)*】タブでは、FTPプロキシの透過モードをスキップできるホストとネットワークを指定できます。

注 - FTPプロキシは、Active Directory認証を使用するFTPサーバとは通信できません。FTPクライアントがこのようなFTPサーバに接続できるようにするには、このサーバをFTPプロキシのスキップリストに追加します。

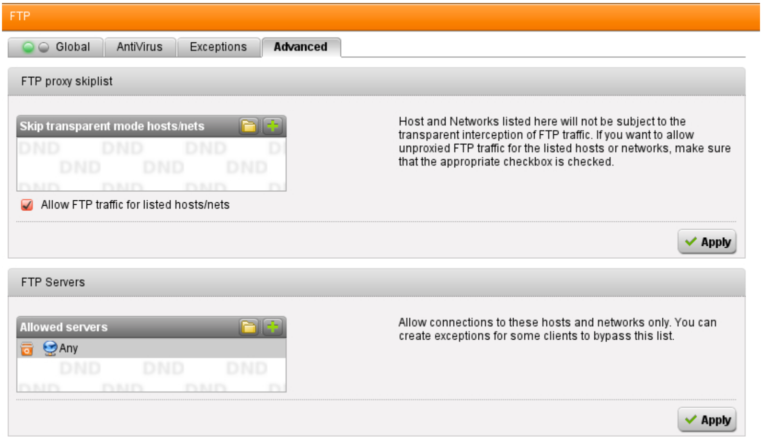


図89 FTPプロキシ(FTP Proxy):詳細設定

FTPプロキシスキップリスト(FTP Proxy Skiplist)

ここにリストされたホストとネットワークは、FTPトラフィックの透過的なインターセプションから除外されます。これらのホストとネットワークに対してFTPトラフィックを許可するには、*【FTPトラフィックを許可(Allow FTP Traffic)】*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

FTPサーバ(FTP Servers)

ネットワークからのアクセスを許可するFTPサーバを選択または追加します。一部のクライアントがこのリストをバイパスするように、*【除外(Exceptions)】*タブで除外ルールを作成できます。

10メールセキュリティ

この章では、Astaro Security Gatewayの基本的なEメールセキュリティ機能の設定方法について説明します。WebAdminの【*メールセキュリティ統計(Mail Security Statistics)*】ページには、Eメール送信者、Eメール受信者、スパマ(国別)、認識されたマルウェア、同時接続の概要が、今日の上位10件まで表示されます。各セクションには、【*詳細(Detail)*】リンクが含まれています。リンクをクリックするとWebAdminのそれぞれのレポーティングセクションが表示され、そこでさらなる統計情報を参照できます。

この章には次のトピックが含まれます。

- SMTP
- SMTPプロファイル
- POP3
- 暗号化
- 隔離レポート
- メールマネージャ

10.1SMTP

【*メールセキュリティ(Mail Security)*】>>【*SMTP*】メニューでSMTPプロキシを設定できます。SMTPは*簡易メール転送プロトコル(Simple Mail Transfer Protocol)*の略で、Eメールをメールサーバに転送するために使用されるプロトコルです。Astaro Security Gateway はSMTPのためのアプリケーションレベルのゲートウェイを装備しており、これを使用して内部メールサーバをリモートの攻撃から守り、さらに強力なウイルススキャンおよびEメールフィルタサービスを提供できます。

注 - SMTPプロキシを正しく使用するには、有効なネームサーバ(DNS)を設定する必要があります。

10.1.1グローバル

【*メールセキュリティ(Mail Security)*】>>【*SMTP*】>>【*グローバル(Global)*】タブで、SMTP設定に対して【*シンプルモード(Simple Mode)*】を使用するか【*プロファイルモード(Profile Mode)*】を使用するかを決定できます。

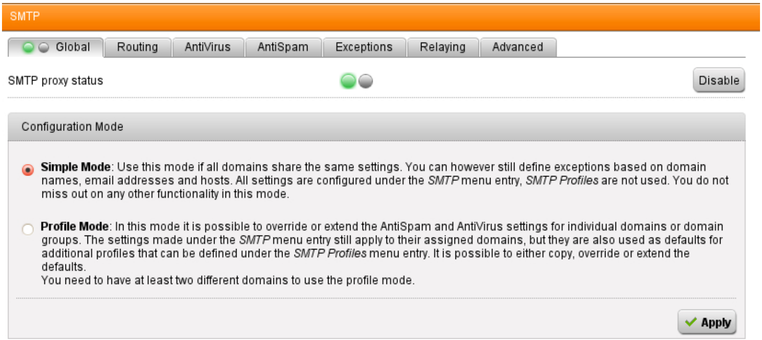


図90 SMTPプロキシ(SMTP Proxy):SMTPプロキシの有効化

1. **SMTPを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンが緑色に変わり【*設定モード(Configuration Mode)*】エリアが編集可能になります。

2. **設定モードを選択します。**
   シンプルモード(Simple Mode): すべてのドメインが同じ設定を共有している場合はこのモードを使用します。ただし、ドメイン名、Eメールアドレス、およびホストに基づいて除外ルールを定義することもできます。これは【*プロファイルモード(Profile Mode)*】と異なり機能的な制限はありません。

   プロファイルモード(Profile Mode): このモードでは、個々のドメインあるいはドメイングループのアンチスパムやアンチウイルスなどのグローバル設定を、【*SMTPプロファイル(SMTP Profiles)*】メニューでそれらのプロファイルを作成することで、上書きまたは拡張できます。【*SMTP*】メニューで行った設定は、依然として指定のドメインに適用され、プロファイルのデフォルトとなります。【*プロファイルモード(Profile Mode)*】には、当製品のプロファイルモードや動作の推奨設定について、いくつかの注意事項があります。ASG.

3. **【*適用(Apply)*】をクリックします。**
   選択したモードが有効になります。

10.1.2ルーティング

【*ルーティング(Routing)*】タブで、SMTP プロキシのドメインとルーティングターゲットを設定し、受信者の確認方法を定義できます。

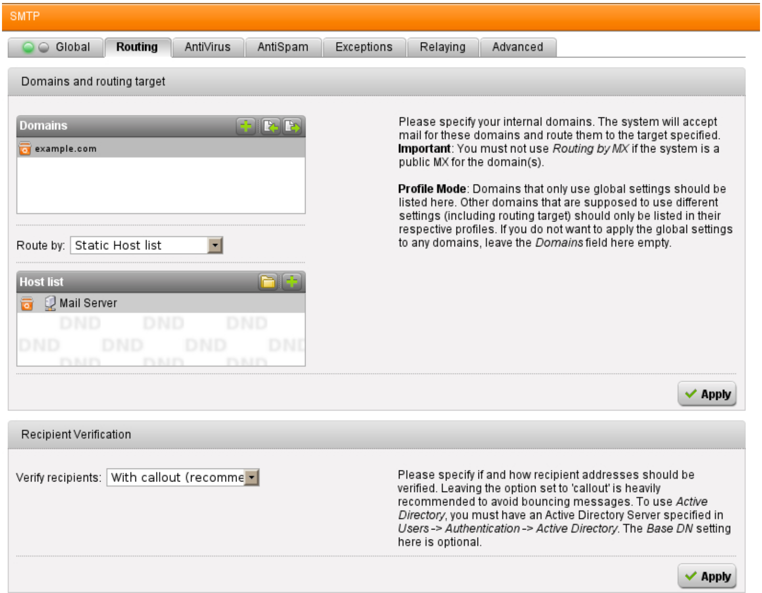


図91 SMTPプロキシ(SMTP Proxy):ドメインとルーティングターゲットの設定

SMTPプロキシのルーティングを設定するには、以下の手順に従います。

1. **内部ドメインを入力します。**
   Eメールのドメインを入力するには、*【ドメイン(Domains)】*ボックスの「+」アイコンをクリックします。

   表示されたテキストボックスに、`example.com`の形式でドメインを入力し、*【適用(Apply)】*をクリックします。すべてのドメインがリストされるまでこのステップを繰り返します。

   プロファイルモード(In Profile Mode):グローバル設定を使用するドメインのみを入力します。他のすべてのドメインは、それぞれのプロファイルにリストします。

2. **内部サーバを指定します。**
   *【ルート毎(Route By)】*ドロップダウンリストで、上記でリストしたドメイン宛てのEメールの転送先ホストを選択します。一般的なターゲットホストとしては、ローカルネットワーク上のMicrosoft Exchange Serverが挙げられます。さまざまなサーバタイプから選択できます。

   - **スタティックホストリスト(Static Host List)**:*【ホストリスト(Host List)】*ボックスで、ターゲットルートのホスト定義を選択します。基本的なフェイルオーバー用に複

数のホスト定義を選択できます。最初のホストへの配信に失敗すると、メールは次のホストにルーティングされます。ただし、ホストのスタティック(静的)な順序は、現在のバージョンのAstaro Security Gatewayでは決定できず、やや偶発的に決定されます。基本的な負荷分散機能をさらに効率よく達成できるようにホストグループへの配信をランダム化するには、【*DNSホスト名(DNS Hostname)*】ルートタイプを使用し、複数のAレコードを持つホスト名を指定します(*Aレコード*または*アドレスレコード*は、ホスト名をIPアドレスにマップします)。

- **DNSホスト名(DNS Hostname)**: ターゲットルートの*完全修飾ドメイン名*(FQDN)を指定します(例:`exchange.example.com`)。複数のAレコードを持つDNS名を選択すると、各サーバへのメールはランダムに配信されます。さらに、1台のサーバに障害が発生すると、そのサーバ宛てのすべてのメールは残りのサーバに自動的にルーティングされます。

- **MXレコード(MX Records)**: MXレコードを使用して、お使いのドメインにメールをルーティングすることもできます。このルートタイプを選択すると、Astaro Security Gatewayのメール転送エージェントは、受信者のドメイン名(Eメールアドレスの"@"文字に続く部分)のMXレコードを要求するDNSクエリを行います。ゲートウェイが上記で指定したドメインのプライマリMXではないことを確認する必要があります。なぜなら、自らにはメールを配信しないからです。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

受信者の確認

受信者を確認(Verify recipients): ここでEメール受信者を確認するかどうかと確認方法を指定できます。

- **コールアウト使用(With Callout)**: 受信者確認の要求がサーバに送信されます。

- **Active Directory**: 受信者確認の要求がActive Directoryサーバに送信されます。Active Directoryを使用するには、【*定義およびユーザ(Definitions & Users)*】>>【*認証サーバ(Authentication Servers)*】&【*サーバ(Servers)*】で指定されたActive Directoryサーバを備えていることが必要です。ベースDNを【*代替ベースDN(Alternate Base DN)*】フィールドに入力します。

> **注 -** Active Directory受信者検証を使用すると、サーバが応答しない場合にメッセージがバウンスされる場合があります。

- **オフ(Off)**: 受信者確認は完全にオフにできますが、推奨されません。なぜなら、オフにすると、スパムトラフィックが増大して、辞書攻撃の危険性が高まるからです。この結果、隔離場所が迷惑メールで溢れてしまうことになります。

設定を保存するには【*適用(Apply)*】をクリックします。

10.1.3アンチウイルス

【*アンチウイルス(AntiVirus)*】タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを含むEメールに対するさまざまな対策が含まれています。

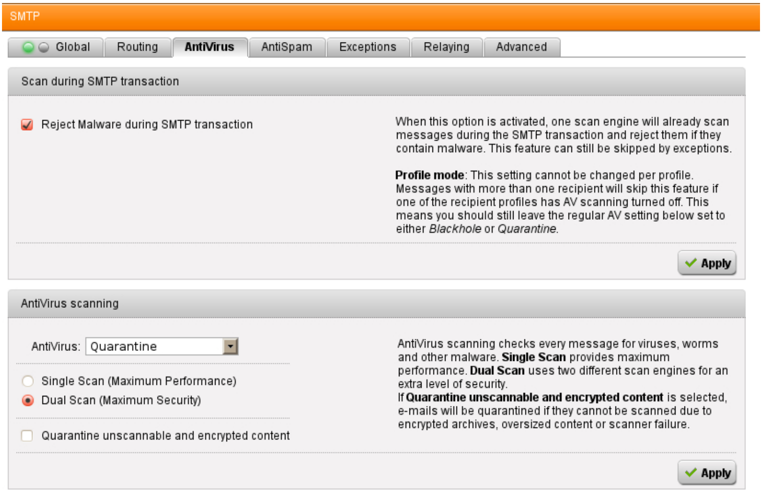


図92 SMTPプロキシ(SMTP Proxy):アンチウイルス設定の構成

SMTPトランザクション時にスキャン(Scan During SMTP Transaction)

【*SMTPトランザクション時にマルウェアをリジェクト(Reject Malware During SMTP Transaction)*】チェックボックスにチェックを入れることで、SMTPトランザクション中にスキャンを行い、マルウェアが含まれている場合は拒否(リジェクト)することができます。

プロファイルモード(In Profile Mode): この設定はプロファイルごとには変更できません。1人以上の受信者がいるメッセージで、受信者の1人のプロファイルで【*アンチウイルススキャン(AntiVirus Scanning)*】がオフになっている場合は、この機能はスキップされます。したがって、以下の通常のアンチウイルス設定を【*ブラックホール(Blackhole)*】あるいは【*隔離(Quarantine)*】のいずれかの設定にしておくことをお勧めします。

設定を保存するには【*適用(Apply)*】をクリックします。

アンチウイルススキャン(AntiVirus Scanning)

このオプションでは、ウイルス、トロイの木馬、疑わしいファイルタイプなどの不要なコンテンツがないかどうか、Eメールをスキャンします。悪意のあるコンテンツを含むメッセージはブロックされて、Eメールの隔離場所に保存されます。ユーザは、Astaroユーザポータルまたはデイリーの隔離レポートで、隔離されたメッセージを確認してリリースできます。ただし、悪意のあるコンテンツを含むメッセージは、メールマネージャで管理者のみが隔離からリリースできます。

アンチウイルス(AntiVirus): 悪意あるコンテンツを含むメッセージの処理方法を設定できます。次の作業を実行できます。

- **オフ(Off)**: アンチウイルススキャンを実行しません。
- **ブラックホール(Blackhole):** メッセージは受信後、ただちに削除されます。
- **隔離(Quarantine)**: メッセージはブロックされ、Eメールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。悪意のあるコンテンツを含むメッセージを隔離場所からリリースできるのは、管理者だけです。

Astaro Security Gateway は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン(Single Scan)**: デフォルトの設定で、最高のパフォーマンスを提供します。
- **デュアルスキャン(Dual Scan)**: 異なるウイルススキャナを使用してすべてのEメールを2回スキャンすることで最大の認識率を提供します。

スキャン不可コンテンツと暗号化コンテンツを隔離(Quarantine Unscannable and Encrypted Content): このオプションを選択して、コンテンツをスキャンできたEメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

設定を保存するには【*適用(Apply)*】をクリックします。

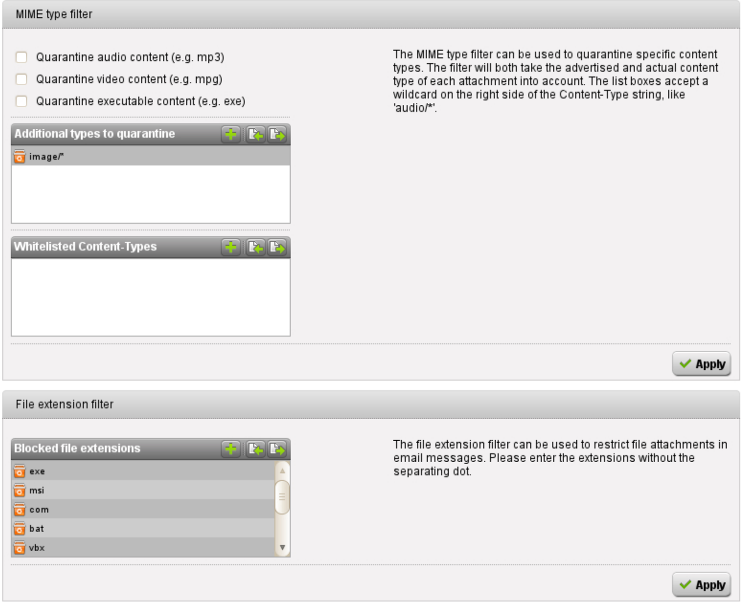


図93 SMTPプロキシ(SMTP Proxy):ファイル拡張子フィルタ(File Extension Filter)

MIMEタイプフィルタ(MIME Type Filter)

MIMEタイプのフィルタはMIMEタイプのEメールコンテンツを読みます。さまざまなMIMEタイプをどう取り扱うかを定義できます。

- **音声コンテンツを隔離(Quarantine Audio Content)**: このチェックボックスにチェックを入れると、mp3あるいはwavファイルなどの音声コンテンツが隔離されます。
- **動画コンテンツを隔離(Quarantine Video Content)**: このチェックボックスにチェックを入れると、mpgあるいはmovファイルなどの動画コンテンツが隔離されます。
- **実行可能ファイルコンテンツを隔離(Quarantine Executable Content)**: このチェックボックスにチェックを入れると、exeファイルなどの実行可能ファイルコンテンツが隔離されます。

隔離する他のタイプ(Additional Types To Quarantine): 上記以外のMIME タイプを隔離するには、【*隔離する他のタイプ(Additional Types To Quarantine)*】ボックスの「+」アイコンをクリックし、MIMEタイプ(例:`image/gif`)を入力します。スラッシュ右側にワイルドカード(`*`)を使用できます(例:`application/*`)。

ホワイトリストのコンテンツタイプ(Whitelisted Content-Types): このボックスを使用して一般的に信頼できるMIMEタイプを許可します。MIMEタイプを追加するには【*ホワイトリストのコンテ*

ンツタイプ(Whitelisted Content-Types)】ボックスの「+」アイコンをクリックし、MIMEタイプを入力します。

MIMEタイプ	MIMEタイプのクラス
audio/*	音声ファイル
video/*	動画ファイル
application/x-dosexec	アプリケーション
application/x-msdownload	
application/exe	
application/x-exe	
application/dos-exe	
vms/exe	
application/x-winexe	
application/msdos-windows	
application/x-msdos-program	

表2: MIMEタイプフィルタで認識されるMIMEタイプ

表3: 設定を保存するには【*適用(Apply)*】をクリックします。

ファイル拡張子フィルタ(File Extension Filter)

この機能は、ファイル拡張子に基づいて特定タイプのファイル(実行可能ファイルなど)を含むEメールを(警告付きで)フィルタリングし、隔離します。ファイル拡張子を追加するには、【*ブロックするファイル拡張子(Blocked File Extensions)*】ボックスの「+」アイコンをクリックし、スキャンするファイル拡張子(例:`exe`、`jar`(区切り文字のドットなし))を入力します。設定を保存するには【*適用(Apply)*】をクリックします。

> **注 -** 暗号化された`zip`アーカイブは、悪意あるコンテンツについてスキャンすることはできず、ウイルススキャナを通過します。暗号化された`zip`ファイルに含まれるマルウェアからネットワークを保護するために、`zip`ファイル拡張子をすべてブロックすることを検討してください。

アンチウイルスチェックフッタ

各送信メールで、悪意あるコンテンツについてEメールをスキャン済みであることをユーザに知らせる特別なフッタを追加してカスタマイズできます。ただし、アンチウイルスチェックフッタは、Eメールが

返信の場合(*In-Reply-To*ヘッダを持つもの)またはEメールのコンテンツタイプを判定できない場合は、Eメールに追加されません。設定を保存するには【*適用(Apply)*】をクリックします。

注 -Eメールクライアント(例:Microsoft OutlookまたはMozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、アンチウイルスチェックフッタオプションを無効にしてください。ただし、Eメール通信のプライバシや認証を保ちながら一般的なアンチウイルスチェックフッタを使用したい場合は、Astaro Security Gatewayの組み込みEメール暗号化機能を使用してください。ゲートウェイ上でのEメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

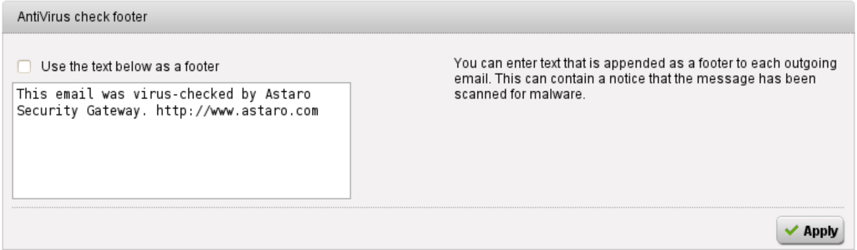


図94 SMTPプロキシ(SMTP Proxy):アンチウイルスチェックフッタ

10.1.4アンチスパム

Astaro Security Gateway を設定して、未承諾のスパムメールを検出したり、既知の(または疑わしい)スパム発信者からのスパム送信を特定することができます。【*アンチスパム(AntiSpam)*】タブにある設定オプションを使用して、SMTPのセキュリティ機能を設定し、未承諾の宣伝用Eメールなどからネットワークを保護します。

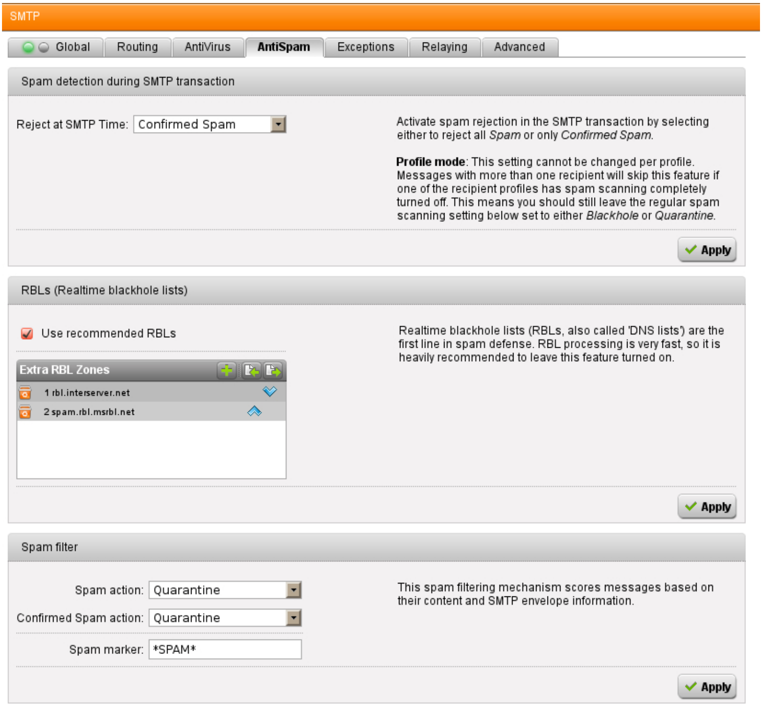


図95 SMTPプロキシ(SMTP Proxy):アンチスパム設定の構成

注 –SMTPプロキシのアンチスパムエンジンによってスキャンされるメッセージの最大サイズは128KBです。このサイズを超えるメッセージにはスパムのスキャンが行われません。

SMTPトランザクション中のスパム検出(Spam Detection During SMTP Transaction)

SMTPトランザクション中にスパムを拒否することができます。【*SMTP時にリジェクト(Reject at SMTP Time)*】オプションに、次のいずれかの設定を選択します。

- **オフ(Off)**: スパム検出は無効となり、スパムが原因でEメールが拒否されることは一切ありません。
- **確認されたスパム(Confirmed Spam)**: 確認されたスパムのみ拒否されます。
- **スパム(Spam)**: システムがスパムとみなす全てのEメールが拒否されます。ニュースレターなどのEメールを、スパムの疑いがあるとみなして却下する場合もあるため、誤検出率が高くなる可能性があります。

プロファイルモード(In Profile Mode): この設定はプロファイルごとには変更できません。メッセージが複数の受信者宛てであり、いずれかの受信者のプロファイルでスパムのスキャンが完全にオフになっている場合、この機能は省略されます。つまり、通常のスパムスキャン設定を【*スパム(Spam)*】または【*確認されたスパム(Confirmed Spam)*】のいずれかにしておくことをお勧めします。

RBL(リアルタイムブラックホールリスト)

リアルタイムブラックホールリスト(RBL)とは、スパム行為に関連しているIPアドレスのリストをインターネットサイトが公開する方式です。

推奨されたRBLを使用(Use Recommended RBLs): このオプションを選択すると、メール転送エージェントは外部のデータベースに対して既知のスパム送信者(いわゆる*リアルタイムブラックホールリスト*)を問い合わせます。あるサイトが、それらのリストの1つ以上に含まれていれば、このサイトからの送信メッセージを容易に拒否することができます。このようなサービスの一部はインターネットで利用できます。この機能を使用することにより、スパムを大幅に減らすことができます。

デフォルトで、以下のRBLに対して問い合わせます。

- Commtouch IP Reputation(ctipd.org)
- cbl.abuseat.org

注 -Astaro Security Gateway が問い合わせるRBLリストは、予告なしに変更される場合があります。Astaroは、これらのデータベースの内容を保証しません。

Astaro Security Gatewayのアンチスパム機能を強化するために、さらなるRBLサイトを追加して、アンチスパム機能を強化できます。追加するには、【*追加のRBLゾーン(Extra RBL Zones)*】ボックスでプラスアイコンをクリックします。表示されたテキストボックスにRBLゾーンを入力します。

設定を保存するには【*適用(Apply)*】をクリックします。

スパムフィルタ(Spam Filter)

Astaro Security Gateway には、スパムの特徴がある受信Eメールをヒューリスティックに(発見的方法で)チェックする機能があります。この機能は、SMTPエンベロープ情報と、発見的テストおよび特性に関する内部データベースを使用します。このスパムフィルタオプションでは、メッセージの内容とSMTPエンベロープ情報に基づいてメッセージにスコアを付けます。スコアが高いほど、スパムの可能性が高いことを意味します。

次の2つのオプションを使用して、ある一定のスパムスコアが付いたメッセージへの対応方法を指定することができます。これにより、スパムの可能性があるEメールに、ゲートウェイが特別に対応できるようになります。

- **スパム対策(Spam Action)**: ここでは、スパムの可能性があるとして分類されたメッセージに対する対策を定義できます。ここでは、誤検出、つまり、ニュースレターなどが間違ってスパムに分類され、ブラックホール化によってEメールが紛失する場合があることに注意してください。
- **確認されたスパムへの対策(Confirmed Spam Action)**: ここでは、スパムと確認されたメッセージに対する対策を定義できます。

これら2種類のスパムに対する処理を、さまざまな対策から選択できます。

- **オフ(Off)**: メッセージはスパムとしてマークされたり、フィルタされません。
- **警告(Warn)**: メッセージはフィルタされません。その代わりに、スパムフラグがメッセージヘッダに追加され、スパムマーカがメッセージの件名に追加されます。
- **隔離(Quarantine)**: メッセージはブロックされ、Eメールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。
- **ブラックホール(Blackhole):** メッセージは受信後、ただちに削除されます。

スパムマーカ(Spam Marker): このオプションで、スパムマーカを指定できます。スパムマーカとは、スパムメッセージをすばやく簡単に識別できるように、メッセージの件名行に追加される文字列です。デフォルトでは、スパムメッセージを示すために`*SPAM*`という文字列が使用されます。

送信者ブラックリスト(Sender Blacklist)

受信SMTPセッションのエンベロープ送信者は、このブラックリスト内のアドレスと照合されます。エンベロープ送信者がブラックリストに含まれている場合、メッセージはブラックホール化されます。ブラックリストに新しいアドレスパターンを追加するには、【*ブラックリストアドレスパターン(Blacklisted Address Pattern)*】ボックスでプラスアイコンをクリックし、アドレス(の一部)を入力してから、【*適用(Apply)*】をクリックします。ワイルドカードとしてアスタリスク(*)を使用できます(例:`*@abbeybnknational.com`)。

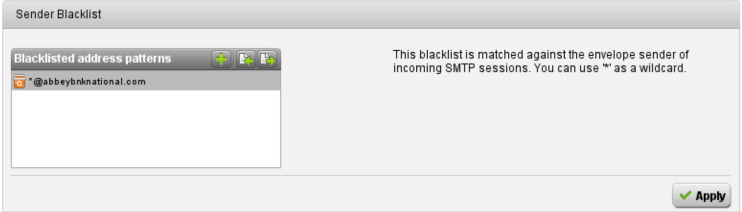


図96 SMTPプロキシ(SMTP Proxy):送信者ブラックリストを拡張する

表現フィルタ(Expression Filter)

表現フィルタは、SMTPプロキシを通過するメッセージに特定の表現が含まれていないか、コンテンツをスキャンし、疑いのあるEメールをブロックします。表現は*Perl互換の正規表現*で指定できます。たとえば、「online dating」などの簡単な文字列は、大文字と小文字を区別しないで解釈されます。設定を保存するには**[*適用(Apply)*]**をクリックします。

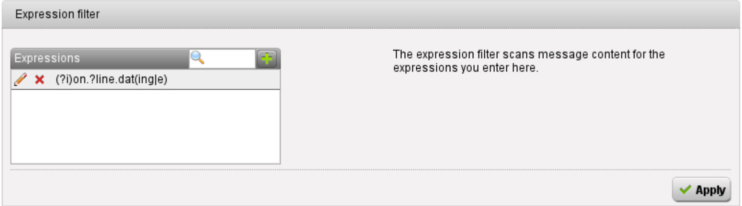


図97 SMTPプロキシ(SMTP Proxy):表現フィルタに表現を追加する

高度なアンチウイルス機能

このエリアには、Astaro Security Gatewayのアンチスパム機能を強化するために、次のような他のさまざまな高度なオプションを使用できます。

無効なHELO/RDNS不足のリジェクト(Reject Invalid HELO/Missing RDNS): 無効なHELO エントリを送信するホストやRDNSエントリが不足しているホストを拒否 するには、このオプションを選択します。このチェックからホストを除外するには、**[*除外(Exceptions)*]**タブを使用してください。

グレーリスト化を使用(Use Greylisting): グレーリスト化とは、基本的に、特定の期間にわたってEメールを一時的に拒否することです。一般に、グレーリスト化を使用しているメールサーバは、すべての受信メールから「*トリプレット*」と呼ばれる3種類の情報を記録します。

- 送信者のアドレス
- メッセージ送信元のホストのIPアドレス
- 受信者のアドレス
- メッセージ件名

このトリプレットは、SMTPプロキシの内部データベースと照合してチェックされます。新しいトリプレットが見つかった場合には、それを記述する特別なタイムスタンプとともにデータベースに記録が作成されます。このトリプレットにより、当該Eメールが5分間にわたって拒否されます。5分経つとプロキシがトリプレットを認識します。当該メッセージが再送信されると、このメッセージは許可されます。トリプレットは、1週間以内に更新されなければ、1週間後に失効します。
グレーリスト化では、ほとんどのスパムメッセージ送信者が「fire-and-forget」方式を使用している点を利用しています。これは「メールを送りつけて、うまくいかなければ忘れる」という方式です。つまり、RFC準拠のメールサーバと違い、スパムメール送信者は、一時的な失敗が発生したEメールを再送信しません。この機能では、次のことが前提となっています。つまり、一時的な失敗はEメール配信に関するRFC仕様に起因するため、正当なサーバは後でEメールを再送信します。その時点で宛先にEメールが受け入れられます。

BATVを使用(Use BATV): BATVとは、Eメールアドレスの正当な使用と不正な使用を区別することを目指すIETFの草稿です。BATVは、簡単な共有鍵を追加してアドレス、時変情報、および任意のランダムデータのハッシュを符号化することにより、送信メールのエンベロープ送信者に署名を施して、Eメールが本当に送信者からのものであると証明する方法を提供します。これは主に、送信者自身が送信したものではないバウンスメールを拒否するために使用されます。BATVを使用することにより、受信するバウンスが本当に自分が送信したEメールに由来しており、スパム送信者が偽造したアドレスからのEメールではないことを確認できるようになります。戻ってきたバウンスメールのEメールアドレスがBATVに従って署名されていない場合、SMTPプロキシはこのメッセージを受け付けません。BATVによる署名は7日後に失効します。Eメールのエンベロープ`MAIL FROM`アドレスのハッシュを符号化するために使用する鍵(別名「*BATVシークレット*」)を変更するには、**【***メールセキュリティ(Mail Security)***】**>>**【***SMTP***】**>>**【***詳細(Advanced)***】**タブに進みます。

> **注 -** メール転送エージェントによっては、BATVによってエンベロープ送信者アドレスが変更されたメッセージを拒否する場合があります。この場合、影響を受ける送信者、受信者、ドメインに対して除外ルールを作成する必要があります。

SPFチェックを実施(Perform SPF check): SPF(*送信者ポリシフレームワーク:Sender Policy Framework*)とは、ドメインの所有者が送信Eメールサーバに関する情報を公開するためのフレームワークです。ドメインは公開レコードを使用して、さまざまなサービス(Web、Eメールなど)をこれらのサービスを実行するマシンに送信します。すべてのドメインは、そのドメインへのメールをどのマシンが受信するのかを知らせるMXレコードをEメール関連のサービス用に公開しています。SPFでは、ドメインからある種の「リバースMXレコード」を公開することにより、そのドメインからのメールを送信しているマシンを広く一般に伝えます。特定のドメインからメッセージを受信すると、受信者はそれらのレコードを確認して、正当な送信者からのメールであることを確認します。

クロスリファレンス- 詳細は、送信者ポリシフレームワーク(Sender Policy Framework)Webサイトでご確認ください。

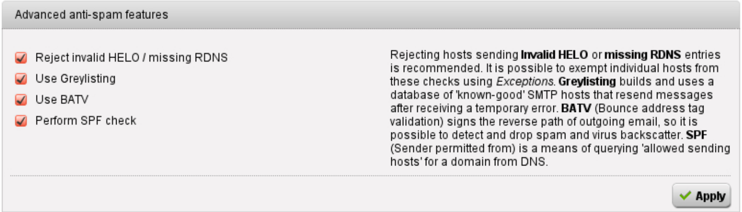


図98 SMTPプロキシ(SMTP Proxy):高度なアンチウイルス機能

追加のアンチスパム機能として、SMTPプロキシは、任意のアドレスへのメールを受信したときに、バックエンドのメールサーバに対して受信者アドレスを暗黙でチェックしてからそのメールを受け付けます。無効な受信者アドレスへのEメールは許可されません。この機能が動作するためには、使用しているバックエンドメールサーバが、SMTPステージで不明受信者へのメールを拒否できなければなりません。原則的に、バックエンドサーバがメッセージを拒否すれば、SMTPプロキシもこのメッセージを拒否します。

ただし、受信者の確認は信頼される(許可される)ホストやリレーホストに対しては*行われません*。この理由は、ユーザエージェントによっては、SMTPトランザクションで受信者が拒否されると問題が発生する場合があるためです。一般的なシナリオ(バックエンドメールサーバがSMTPトランザクションで不明な受信者を拒否する)では、Astaro Security Gateway バウンスが生成されるのは次の場合に限られます。

- 信頼される送信元やリレー元が、配信不能な受信者にメッセージを送信した場合。
- バックエンドメールサーバが停止しており、Astaro Security Gateway 受信者を確認できなかった場合。

ただし、Astaro Security Gateway は、バックエンドメールサーバからの配信不能レポート(NDR)やバウンスの送信を防止することはできません。さらに、Astaro Security Gateway は、メールサーバからのスパムの可能性のあるコールアウト応答は24時間キャッシュし、可能性のないものは2日間キャッシュします。

10.1.5除外

*【SMTP】>>【除外(Exceptions)】*タブで、アンチスパム、アンチウイルス、またはその他のセキュリティチェックから除外するホワイトリストのホスト、ネットワーク、送信者、および受信者を定義で

きます。

注 - Eメールは多数の受信者に送信される場合がありますが、Astaro Security GatewayはSMTPプロトコルのインラインスキャニングを実装しているため、Eメール受信者のうち1人でも【*受信者(Recipeints)*】ボックスにリストされていると、Eメールのスキャンはすべての受信者に対してスキップされます。

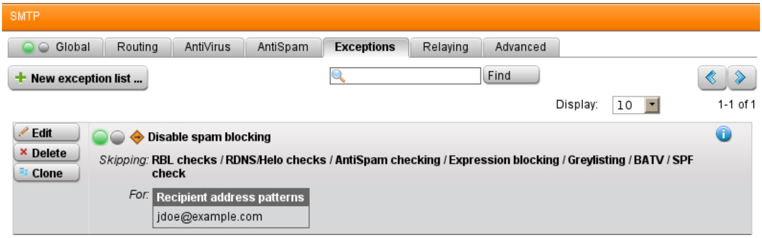


図99 SMTPプロキシ(SMTP Proxy):除外リスト

除外ルールを作成するには、次の手順に従います。

1. ***【除外(Exception)】タブで、【新規除外リスト(New Exception List)】をクリックします。***
   【*除外リストを作成(Create Exception List)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name):この除外を説明する名前を入力します。

   スキップするチェック(Skip These Checks):スキップするセキュリティチェックを選択します。詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*アンチウイルス*」および「*アンチスパム*」を参照してください。

   スキップする送信元ホスト/ネットワーク(For These Source Hosts/Networks):この除外ルールで定義されたセキュリティチェックをスキップする送信元ホスト/ネットワーク(メッセージが発信されたホストまたはネットワーク)を選択します。

   注 - ローカルメッセージはデフォルトでスキャンされないので、ローカルホストには除外を作成する必要はありません。

   このオプションを選択すると、【*ホスト/ネットワーク(Hosts/Networks)*】ダイアログボックスが開きます。「+」記号またはフォルダ記号をクリックして、ホストあるいはネットワークを追加できます。

送信者アドレスで除外(These Sender Addresses): 定義したセキュリティチェックをスキップする送信者のEメールアドレスを選択します。
このオプションを選択すると、【*送信者(Senders)*】ダイアログボックスが開きます。完全で有効なEメールアドレスを入力するか(例: `jdoe@example.com`)、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのEメールアドレスを指定できます(例: `*@example.com`)。

> **注 -** 送信者アドレスは容易に偽造できるため、【*送信者(Senders)*】オプションを使用する際は注意が必要です。

スキップする受信者アドレス(These Recipient Addresses): 定義されたセキュリティチェックをスキップする受信者のEメールアドレスを選択します。

このオプションを選択すると、【*受信者(Recipients)*】ダイアログボックスが開きます。完全で有効なEメールアドレスを入力するか(例: `jdoe@example.com`)、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのEメールアドレスを指定できます(例: `*@example.com`)。

コメント(Comment)(オプション): 説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。** 新しい除外が【*除外(Exceptions)*】リストに表示されます。

例外を編集または削除するには、対応するボタンをクリックします。

10.1.6リレー

SMTPプロキシはメールリレーとして使用できます。メールリレーは、特定のユーザ、ユーザグループ、あるいはホストがそれを介してローカル以外のドメインにEメールをリレー(送信)できるように設定されたSMTP サーバです。

アップストリームホストリスト(Upstream Host List)

アップストリームのホストは、Eメールをお客様のISP あるいは外部MXに転送するホストです。スタティックなアップストリームのホストからEメールを受信する場合は、ここにホストを入力する必要があります。ホストを入力しないと、スパム保護が正常に機能しなくなります。

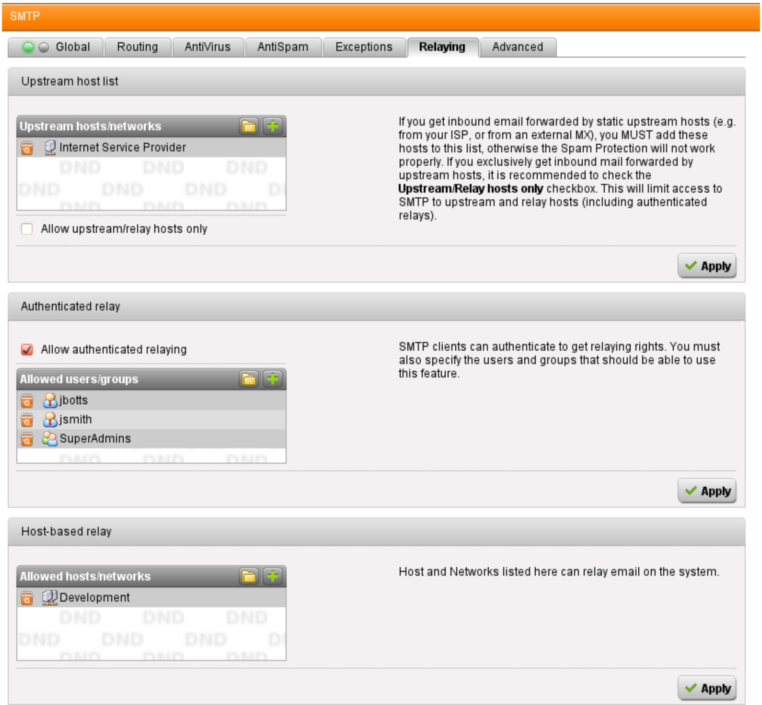


図100 SMTPプロキシ(SMTP Proxy):リレーの設定

アップストリームホストを追加するには、「+」アイコンまたはフォルダアイコンをクリックして、【*ネットワーク(Networks)*】オブジェクトリストからドラッグ&ドロップします。アップストリームホストのみを許可する場合は、【*アップストリーム/リレーホストのみ許可(Allow Upstream/Relay Hosts Only)*】チェックボックスにチェックを入れます。これにより、SMTPアクセスは、定義されたアップストリームホスト(および下記の認証されたリレー)に制限されます。設定を保存するには【*適用(Apply)*】をクリックします。

認証されたリレー(Authenticated Relay)

SMTPクライアントは、リレー特権の取得を認証できます。【*認証されたリレーの許可(Allow Authenticated Relaying)*】チェックボックスにチェックを入れて、この機能を使用できるようにするユーザおよびユーザグループを指定します。設定を保存するには【*適用(Apply)*】をクリックします。

ホストベースのリレー(Host-based Relay)

メールリレーも、ホストベースに対応できます。お使いのローカルメールサーバあるいはメールクライアントがSMTPプロキシをメールリレーとして使用する必要がある場合は、リレーを介してメールを送信できるようにするネットワークやホストを【*許可するホスト/ネットワーク(Allowed Hosts/Networks)*】ボックスに追加する必要があります。リストされたネットワークやホストは、どのアドレスにもメッセージを送信できます。

警告 -【*許可するホスト/ネットワーク(Allowed Hosts/Networks)*】ボックスでは、絶対に【*すべて(Any)*】を選択しないでください。これを選択すると、オープンリレーになり、インターネット上の誰もがSMTPプロキシ経由でメッセージを送信できるようになります。スパマはこれをすぐに見つけ、大量のEメールトラフィックを送信します。最悪の場合は、お客様がサードパーティのスパマブラックリストに載ることになってしまいます。ほとんどの設定では、お客様のネットワークのメールサーバだけを、メールのリレーを許可される唯一のホストとすべきです。

設定を保存するには【*適用(Apply)*】をクリックします。

ホスト/ネットワークのブラックリスト(Host/Network Blacklist)

ここで、SMTPプロキシでブロックするホストおよびネットワークを定義できます。設定を保存するには【*適用(Apply)*】をクリックします。

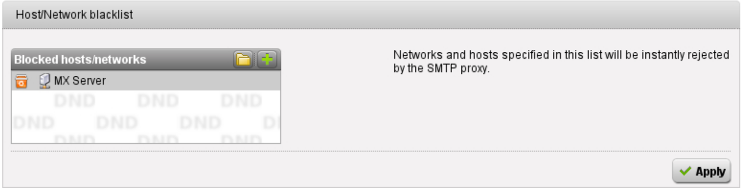


図101 SMTPプロキシ(SMTP Proxy):ホスト/ネットワークのブラックリストの有効化

リレーメッセージのコンテンツをスキャン(Content Scan For Relayed Messages)

このオプションを有効にすると、認証されたリレーあるいはホストベースのリレーで送信されるメッセージについて、悪意あるコンテンツの有無がスキャンされます。送信メールが大量にある場合、このオプションをオフにすると、パフォーマンスが向上します。設定を保存するには【*適用(Apply)*】をクリックします。

送信メッセージには、グローバルなアンチウイルスおよびアンチスパム設定も適用されます。ただし、これらの設定を問わず、感染メッセージやスパムメッセージはブラックホール化ではなく常に隔離されます。これにより、意図しないメールの紛失が回避されます。

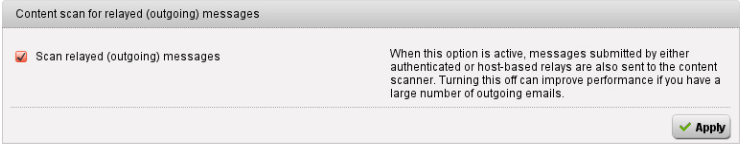


図102 SMTPプロキシ(SMTP Proxy):リレーメッセージのコンテンツスキャンの有効化

10.1.7詳細

*【SMTP】>>【詳細(Advanced)】*タブでは、スマートホストの設定や透過モードスキップリストなどのSMTPプロキシの追加セキュリティオプションを設定できます。

親プロキシ(Parent Proxy)

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国で必要とされます。親プロキシの使用がセキュリティポリシで求められている場合、ここでホスト定義とポートを選択して親プロキシを設定できます。

親プロキシを使用(Use a Parent Proxy): このチェックボックスにチェックを入れて、親プロキシの使用を有効にします。プロキシのホスト名とポートを入力します。

このプロキシは認証が必要(This Proxy Requires Authentication): 親プロキシが認証を必要とする場合は、ここでユーザ名とパスワードを入力します。

透過モード(Transparent Mode)

SMTPの透過モードを有効化するには、チェックボックスにチェックを入れ、*【適用(Apply)】*をクリックします。
*【透過モード時にスキップするホスト/ネット(Skip Transparent Mode Hosts/Nets)】*ボックスにリストされているホストとネットワークは、SMTPトラフィックの透過的インターセプションの対象とはなりません。ただし、これらのホストおよびネットワークでSMTPトラフィックを許可するには、*【リスト内のホスト/ネットワークのSMTPトラフィックを許可(Allow SMTP Traffic For Listed Hosts/Nets)】*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

TLS設定(TLS Settings)

TLS証明書(TLS Certificate): ドロップダウンリストから証明書を選択します。この証明書は、TLS暗号化についてそれをサポートしているすべてのリモートホストとネゴシエートするために使用されます。

TLSネゴシエーションホスト/ネットが必要(Require TLS Negotiation Host/Nets): ここに、Eメール通信のTLS暗号化が常に必要なホストまたはネットを追加します。これにより、ASGは、これらのホスト/ネットで何らかの理由でTLS暗号化を使用できない場合に、Eメールを抑制します。つまり、TLSが使用可能になるまで、メッセージはメールキューに保留されます。一定の期間にわたってTLSを使用できない場合は、送信の試行が停止され、Eメールを送信できなかったという通知がユーザに送信されます。

TLSネゴシエーション送信者ドメインが必要(Require TLS Negotiation Sender Domains): 特定のドメインに対して受信EメールのTLS暗号化を強制するには、ここにドメインを入力します。これらのドメインからTLSなしで送信されたEメールは、即時に拒否されます。

TLSネゴシエーションホスト/ネットをスキップ(Skip TLS Negotiation Host/Nets): 特定のホストやネットワークでTLS暗号化に関する問題が発生した場合は、それをボックスに入力し、適切なTLS証明書をドロップダウンメニューから選択します。それによって、ASGは、このホストまたはネットワークに対するTLSネゴシエーションをスキップします。設定を保存するには【*適用(Apply)*】をクリックします。

送信ドメイン認証技術(DKIM)(Domain Keys Identified Mail (DKIM))

DKIM は発信メッセージに暗号によって署名する方法です。DKIM署名を使用するには、RSA鍵と対応する鍵セレクタを各フィールドに入力し、Eメールに署名するドメインを【*DKIMドメイン(DKIM Domains)*】ボックスに追加します。設定を保存するには【*適用(Apply)*】をクリックします。

機密フッタ(Confidentiality Footer)

各送信メールについて、Eメールに極秘あるいは部外秘の情報が含まれていることなどをユーザに知らせる機密フッタを追加してカスタマイズできます。ただし、機密フッタは、Eメールが返信の場合(例: *In-Reply-To*ヘッダを持つもの)またはEメールのコンテンツタイプを判定できない場合は、Eメールに追加されません。

> **注 -**Eメールクライアント(例:Microsoft OutlookまたはMozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、アンチウイルスチェックフッタオプションを無効にしてください。ただし、Eメール通信のプライバシや認証を保ちながら一般的なアンチウイルスチェックフッタを使用したい場合は、Astaro Security Gatewayの組み込みEメール暗号化機能を使用してください。ゲートウェイ上でのEメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

詳細設定

ここで、SMTPホスト名やポストマスタアドレスなどを設定できます。

SMTPホスト名(SMTP Hostname): SMTPホスト名を設定すると、プロキシは、HELOおよびSMTPバナーメッセージで指定された名前を使用します。デフォルトでは、通常システムのホスト名が選択されています。

ポストマスタアドレス(Postmaster Address): 送信されたメッセージの転送先となるASGのポストマスタのEメールアドレスを`postmaster@[192.168.16.8]`の形で指定します。この場合、IPリテラルアドレスが、ASGのIPアドレスの1つになります。そのようなメッセージを受け入れることがRFC要件となっています。

BATVシークレット(BATV Secret): ここで、SMTPプロキシが使用する、自動的に生成されたBATVシークレットを変更できます。BATVシークレットはEメールのエンベロープの`MailFrom`アドレスへの署名に使用される共有鍵で、無効なバウンスアドレスの検出を可能にします。複数のMXをドメインに使用している場合は、BATVシークレットをすべてのシステムで同じものに変更できます。

最大メッセージサイズ(Max Message Size): プロキシが受け付ける最大メッセージサイズ。この設定は送受信両方のEメールに適用されます。バックエンドサーバにメッセージサイズの制限がある場合は、ここではその制限値以下に設定する必要があります。

最大接続数(Max Connections): プロキシが許可する最大同時接続数。デフォルトは20です。

最大接続/ホスト(Max Connections/Host): プロキシが許可する接続あたりの最大ホスト数。デフォルトは10です。

最大メール/接続(Max Mails/Connection): プロキシが許可する接続あたりの最大メール数。デフォルトは1000です。

最大受信者/メール(Max Rcpt/Mail): プロキシが許可するメールあたりの最大受信者数。デフォルトは500です。

フッタモード(Footers Mode): ここでメールへのフッタの追加方法を定義できます。【*MIMEパート(MIME Part)*】を指定すると、追加のMIMEパートとしてフッタを追加します。既存のパートエンコーディングは変更されないので、国語の文字が保持されます。別の方式である【*インライン(Inline)*】では、フッタがメール本体から区切り記号`--`で分離されます。このモードでは、フッタでUnicode(UTF-8)変換を使用するかどうかを選択できます。Unicode変換を行うと、フッタで国語の文字を保持するようにメッセージがアップグレードされます。

スマートホストの設定(Smarthost Settings)

スマートホストはメールリレーサーバの一種で、SMTPサーバが受信者のサーバに直接メールをルーティングするのではなく、アップストリームのメールサーバにルーティングできるようにします。多くの場合このスマートホストは、送信者がスマートホストを通してメールを送信する権限を持つことを確認するために、送信者の認証を必要とします。

スマートホストを使用する(Use A Smarthost): メールの送信にスマートホストを使用する場合は、このチェックボックスにチェックを入れます。このオプションを選択すると、プロキシ自体がメールを配信することはなくなり、すべてをスマートホストに送信するようになります。

- **スマートホスト(Smarthost)**: スマートホストオブジェクトを選択または追加します。
- **スマートホストポート(Smarthost Port)**: スマートホスト接続のデフォルトポートは25です。必要に応じて、ポートを変更できます。
- **このスマートホストは認証が必要(This Smarthost Requires Authentication)**: スマートホストが認証を必要とする場合は、チェックボックスにチェックを入れます。【*プレーン(Plain)*】と【*ログイン(Login)*】認証タイプの両方がサポートされています。それぞれのフィールドにユーザ名とパスワードを入力します。

10.2SMTPプロファイル

Astaro Security GatewayのSMTPプロキシで、別のSMTPプロファイルを作成し、それを異なるドメインに関連付けることができます。このようにして、【*メールセキュリティ(Mail Security)*】>>【*SMTP*】で設定されたデフォルトのプロファイル以外のプロファイルを使用する特定のドメインを指定できます。機能の順序はタブによって構造化され、SMTPトランザクション時に各ステップが互いにどのように処理されるかを決定します。

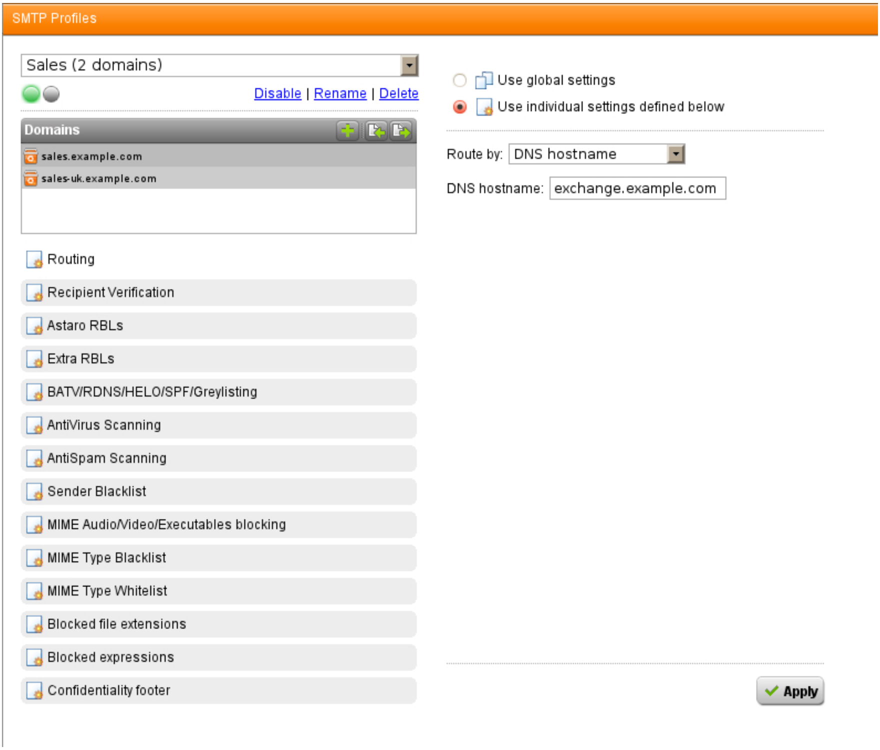


図103 SMTPプロファイル:SMTPプロファイルの設定

SMTPプロファイルを作成するには、以下の手順に従います。

1. **SMTPプロファイルモードを有効にします。**
   【メールセキュリティ(Mail Security)】>>【SMTP】>>【グローバル(Global)】タブで、【プロファイルモード(Profile Mode)】を選択して【適用(Apply)】をクリックします。

   *【メールセキュリティ(Mail Security)】>>【SMTPプロファイル(SMTP Profiles)】メニュー*のSMTPプロファイル作成が有効になります。

2. ***【SMTPプロファイル(SMTP Profiles)】タブで、【新規プロファイルの作成(Create New Profile)】をクリックします。***
   ダイアログボックスが開きます。

3. **プロファイルを説明する名前を入力し、*【OK】*をクリックします。**
   プロファイルの設定ページが開きます。

4. **1つ以上のドメインを追加します。**
   1つ以上のドメインを【*ドメイン(Domains)*】ボックスに追加します。

   このプロファイルの設定が、それらのドメインに適用されます。

5. **次の設定を行います。**
   使用する機能にのみ設定します。以下の各機能に対して、ここで定義する個々の設定を使用するか、または【*メールセキュリティ(Mail Security)*】>>【*SMTP*】で定義するグローバル設定を使用するかを決定できます。デフォルトでは、個々の設定オプションが選択されています。各機能の個々の設定について以下に説明します。

   注 - ここで設定されたドメイン名が送信者アドレスに含まれる暗号化されたEメールは、当製品のEメール暗号化/復号化エンジンを使用しても復号化できません。Astaro Security Gateway. したがって、外部Eメールドメインのプロファイルは含めないようにしてください。

   ここで定義できるすべての設定は、【*メールセキュリティ(Mail Security)*】>>【*SMTP*】でもグローバルに設定できます。したがって、ここでは、設定の一覧とグローバル設定との相違点のみを、対応するグローバル設定へのクロスリファレンスとともに示します。設定の詳細は、グローバル設定でご覧ください。

   以下の設定を行うことができます。

   - **ルーティング(Routing)**:【*ルーティング(Routing)*】タブで、SMTPプロキシのドメインとルーティングターゲットを設定し、受信者の確認方法を定義します。
     - スタティックホストリスト(Static Host List)
     - DNSホスト名(DNS Hostname)
     - MXレコード(MX Records)

     詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*ルーティング*」を参照してください。

   - **受信者の確認**
     受信者を確認(Verify recipients): ここでEメール受信者を確認するかどうかと確認方法を指定できます。

     - **コールアウト使用(With Callout)**: 受信者確認の要求がサーバに送信されます。

     - **Active Directory**: 受信者確認の要求がActive Directoryサーバに送信されます。Active Directoryを使用するには、【*定義およびユー*

ザ(Definitions & Users)】>>【*認証サーバ(Authentication Servers)*】&【*サーバ(Servers)*】で指定されたActive Directoryサーバを備えていることが必要です。ベースDNを【*代替ベースDN(Alternate Base DN)*】フィールドに入力します。

注 - Active Directory受信者検証を使用すると、サーバが応答しない場合にメッセージがバウンスされる場合があります。

- **オフ(Off)**: 受信者確認は完全にオフにできますが、推奨されません。なぜなら、オフにすると、スパムトラフィックが増大して、辞書攻撃の危険性が高まるからです。この結果、隔離場所が迷惑メールで溢れてしまうことになります。

詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*ルーティング*」を参照してください。

- **Astaro RBLおよびダイヤルアップによるブロック(Astaro RBLs and Dial-up Blocking)**: ここでスパムにリンクしたIPアドレスをブロックできます。
  - 推奨されたRBLを使用RBL
  - ダイヤルアップ/レジデンシャルホストのブロック(Block Dial-up/Residential Hosts)

詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*アンチスパム*」を参照してください。

- **追加のRBL(Extra RBLs)**: さらなるRBLサイトを追加して、当製品のアンチスパム機能を強化できます。Astaro Security Gateway. 詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*アンチスパム*」を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。

- **BATV/RDNS/HELO/SPF/グレーリスト化(BATV/RDNS/HELO/SPF/Greylisting)**: このタブでは、当製品のアンチスパム機能を強化するために、次のような他のさまざまな高度なオプションを使用できます。Astaro Security Gateway.
  - 無効なHELO/RDNSなしのリジェクト(Reject Invalid HELO/Missing RDNS)
  - グレーリスト化を使用(Use Greylisting)
  - BATVを使用(Use BATV)
  - SPFチェックを実施(Perform SPF Check)

詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*アンチスパム*」を参照してください。

- **アンチウイルススキャン(AntiVirus Scanning)**: 悪意あるコンテンツを含むメッセージの処理方法を設定できます。次の作業を実行できます。
  - オフ(Off)
  - 隔離(Quarantine)
  - ブラックホール(Blackhole)

  以下のアンチウイルススキャンオプションから選択できます。

  - シングルスキャン(Single Scan):最高のパフォーマンスを提供します。
  - デュアルスキャン(Dual Scan):最大のセキュリティを提供します。

  スキャン不可コンテンツと暗号化コンテンツを隔離(Quarantine Unscannable and Encrypted Content): このオプションを選択して、コンテンツをスキャンできなかったEメールを隔離します。コンテンツをスキャンできなかった理由としては、コンテンツが暗号化されているか、または破損していることが考えられます。

  詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*アンチウイルス*」を参照してください。

- **アンチスパムスキャン(AntiSpam Scanning)**: ここで迷惑な宣伝メールの取り扱いを決めます。スパムおよびスパムと確認されたEメールに対して以下の対策を選択できます。
  - オフ(Off)
  - 警告(Warn)
  - 隔離(Quarantine)
  - ブラックホール(Blackhole)

  詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*アンチスパム*」を参照してください。

- **送信者ブラックリスト(Sender Blacklist)**: 受信SMTPセッションのエンベロープ送信者が、このブラックリストのアドレスと照合されます。エンベロープ送信者がブラックリストに含まれている場合、メッセージはブラックホール化されます。詳細は、「*メールセキュリティ*」>>「*SMTP*」>>「*アンチスパム*」を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。

- **MIME音声/動画/実行可能ファイルのブロック(MIME Audio/Video/Executables Blocking)**:MIME タイプフィルタは、EメールコンテンツのMIMEタイプを読みます。どのタイプのコンテンツを隔離するかを選択できます。

  - 音声コンテンツ
  - 動画コンテンツ
  - 実行可能ファイルコンテンツ

  詳細は、*「メールセキュリティ」>>「SMTP」>>「アンチウイルス」*を参照してください。

- **MIMEタイプのブラックリスト(MIME Type Blacklist)**: ここで、その他のMIMEタイプを隔離場所(検疫)に追加できます。詳細は、*「メールセキュリティ」>>「SMTP」>>「アンチウイルス」*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **MIMEタイプのホワイトリスト(MIME Type Whitelist)**: ここで隔離しないMIMEタイプを追加できます。詳細は、*「メールセキュリティ」>>「SMTP」>>「アンチウイルス」*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **ブロックするファイル拡張子(Blocked File Extensions)**: *ファイル拡張子フィルタ*を使用して、ファイル拡張子に基づいて、特定のファイルタイプ(例:実行可能ファイル)を含むEメールを(警告付きで)隔離できます。詳細は、*「メールセキュリティ」>>「SMTP」>>「アンチウイルス」*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **ブロックする表現(Blocked Expressions)**: 表現フィルタは、SMTPプロキシを通過するメッセージのコンテンツについて、特定の表現をスキャンします。疑いのあるEメールをブロックします。詳細は、*「メールセキュリティ」>>「SMTP」>>「アンチスパム」*を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **機密フッタ(Confidentiality Footer)**:各送信メールについて、Eメールに極秘あるいは部外秘の情報が含まれていることなどをユーザに知らせる機密フッタを追加してカスタマイズできます。ただし、機密フッタは、Eメールが返信の場合(例: *In-Reply-To*ヘッダを持つもの)またはEメールのコンテンツタイプを判定できない場合は、Eメールに追加されません。送信者ドメインに応じて、フッタが追加されます。フッタを使用するには、チェックボックスにチェックを入れ、フッタのテキストを入力して*【適用(Apply)】*をクリックします。

6. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。新しいプロファイルが*【SMTPプロファイル(SMTP Profiles)】*リストに表示されます。

注 -_トピックに【グローバル設定の使用(Use Global Settings)】_を選択して_【適用(Apply)】_をクリックすると、機能のアイコンがグローバル設定のアイコンに変わります。これにより、どの機能に対してグローバル設定または個々の設定が適用されているかが簡単にわかります。

プロファイルの無効化、名前変更、または削除を行う場合は、プロファイルドロップダウンリスト下にある上段の該当するボタンをクリックします。

10.3POP3

_【メールセキュリティ(Mail Security)】>>【POP3】_メニューでは、受信EメールのPOP3プロキシを設定できます。POP3(_Post Office Protocol 3_)はアプリケーション層インターネット標準プロトコルで、リモートメールサーバからのEメールの取り出しを可能にします。POP3プロキシは透過的に機能します。つまり、ポート`110`で内部ネットワークから受信するすべてのPOP3要求は、クライアントには認識されずにプロキシを通してインターセプト(傍受)され、リダイレクトされます。このモードのメリットは、その他の管理やクライアント側の設定が必要ないということです。

注 - 場合によっては、Eメールクライアントの設定でサーバタイムアウト設定を長くすることが必要です。通常のデフォルトである約1分以内の設定では、特に大きなEメールをフェッチするときには短すぎます。

POP3プロトコルには、どのEメールがすでに取り出されたかをサーバ側で追跡する機能はありません。一般的には、メールクライアントがEメールを取り出した後、サーバ上でそれを削除します。ただし、クライアントがメールを削除しないように設定されている場合、サーバ側の削除は行われず、どのメールがすでにフェッチされたかをクライアントが追跡します。

10.3.1グローバル

_【Webセキュリティ(Web Security)】>>【POP3】>>【グローバル(Global)】_タブでは、POP3プロキシの基本設定を構成できます。

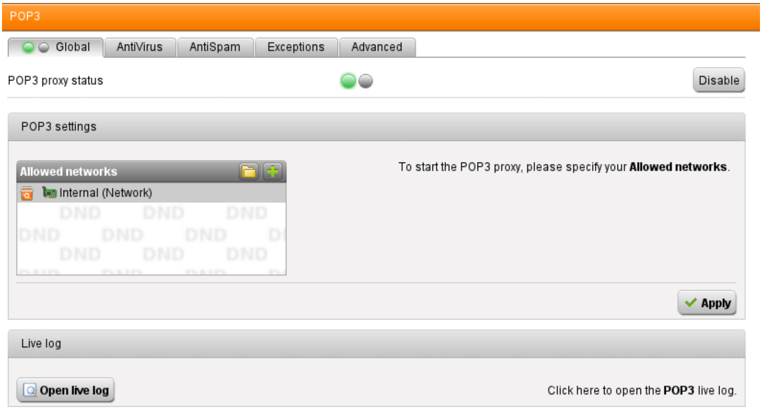


図104 POP3プロキシ(POP3 Proxy):POP3プロキシを有効にする

POP3プロキシを設定するには、以下の手順に従います。

1. **POP3プロキシを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり【*POP3設定(POP3 Settings)*】エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   プロキシPOP3トラフィックに許可するネットワークを選択します。デフォルトでは、これは内部ネットワークです。

3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

設定をキャンセルするには、【*有効化を中止(Abort Enable)*】またはアンバー色のステータスアイコンをクリックします。

ライブログ

*POP3ライブログ(POP3 Live Log)*は、POP3プロキシのアクティビティをログし、すべての受信Eメールを表示します。ボタンをクリックして、新しいウィンドウでライブログを開きます。

10.3.2アンチウイルス

【*アンチウイルス(AntiVirus)*】タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを含むEメールに対するさまざまな対策が含まれています。

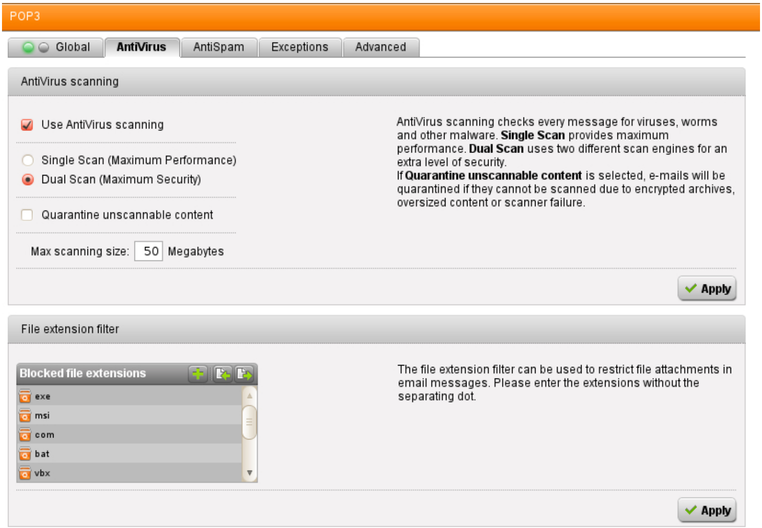


図105 POP3プロキシ(POP3 Proxy):アンチウイルス設定の構成

アンチウイルススキャン(AntiVirus Scanning)

このオプションでは、ウイルス、トロイの木馬、疑わしいファイルタイプなどの不要なコンテンツがないかどうか、Eメールをスキャンします。悪意のあるコンテンツを含むメッセージはブロックされて、Eメールの隔離場所に保存されます。ユーザは、Astaroユーザポータルまたはデイリーの隔離レポートで、隔離されたメッセージを確認してリリースできます。ただし、悪意のあるコンテンツを含むメッセージは、メールマネージャで管理者のみが隔離からリリースできます。

Astaro Security Gateway は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン(Single Scan)**: デフォルトの設定で、最高のパフォーマンスを提供します。
- **デュアルスキャン(Dual Scan)**: 異なるウイルススキャナを使用してすべてのEメールを2回スキャンすることで最大の認識率を提供します。

スキャン不可コンテンツと暗号化コンテンツを隔離(Quarantine Unscannable and Encrypted Content): このオプションを選択して、コンテンツをスキャンできなかったEメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

最大スキャンサイズ(Max Scanning Size): アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

設定を保存するには【*適用(Apply)*】をクリックします。

ファイル拡張子フィルタ(File Extension Filter)

この機能は、ファイル拡張子に基づいて特定タイプのファイル(実行可能ファイルなど)を含むEメールを(警告付きで)フィルタリングし、隔離します。ファイル拡張子を追加するには、【*ブロックするファイル拡張子(Blocked File Extensions)*】ボックスの「+」アイコンをクリックし、スキャンするファイル拡張子(例:`exe`、`jar`(区切り文字のドットなし))を入力します。設定を保存するには【*適用(Apply)*】をクリックします。

注 - 暗号化された`zip`アーカイブは、悪意あるコンテンツについてスキャンすることはできず、ウイルススキャナを通過します。暗号化された`zip`ファイルに含まれるマルウェアからネットワークを保護するために、`zip`ファイル拡張子をすべてブロックすることを検討してください。

10.3.3アンチスパム

Astaro Security Gatewayを設定して、未承諾のスパムメールを検出したり、既知の(または疑わしい)スパム発信者からのスパム送信を特定することができます。【*アンチスパム(AntiSpam)*】タブにある設定オプションを使用して、POP3 セキュリティ機能を設定し、迷惑な宣伝メールをネットワークが受信しないように防止することができます。

注 -POP3プロキシのアンチスパムエンジンによってスキャンされるメッセージの最大サイズは128KBです。このサイズを超えるメッセージにはスパムのスキャンが行われません。

スパムフィルタ(Spam Filter)

Astaro Security Gatewayには、スパムの特徴がある受信Eメールをヒューリスティックに(発見的方法で)チェックする機能があります。スパムフィルタはSMTP エンベロープ情報およびヒューリスティックテストと特徴の内部データベースを使用します。このスパムフィルタオプションでは、メッセージの内容とSMTPエンベロープ情報に基づいてメッセージにスコアを付けます。スコアが高いほど、スパムの可能性が高いことを意味します。

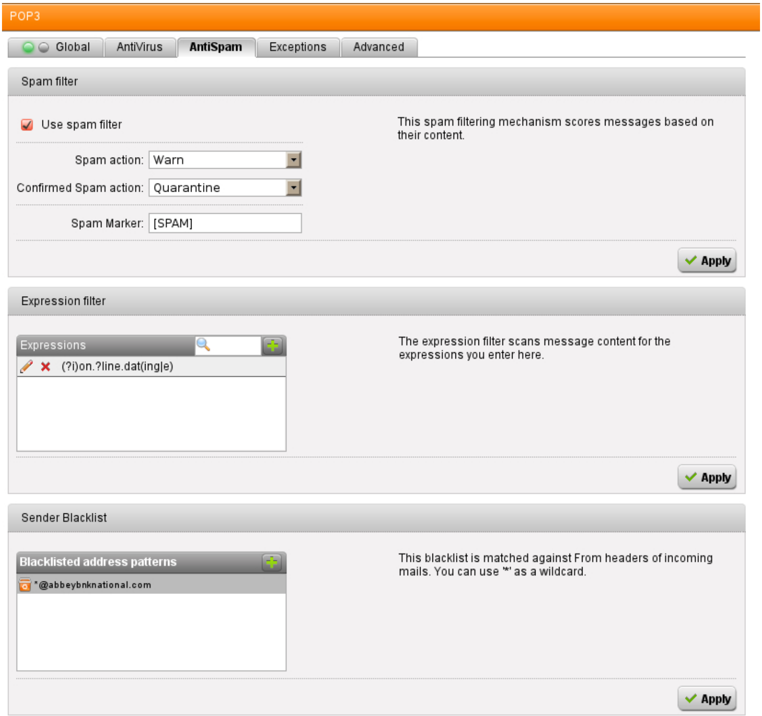


図106 POP3プロキシ(POP3 Proxy):アンチスパム設定の構成

次の2つのオプションを使用して、ある一定のスパムスコアが付いたメッセージへの対応方法を指定することができます。これにより、スパムの可能性があるEメールに、ゲートウェイが特別に対応できるようになります。

- **スパム対策(Spam Action)**: ここでは、スパムの可能性があるとして分類されたメッセージに対する対策を定義できます。ここでは、誤検出、つまり、ニュースレターなどが間違ってスパムに分類され、ブラックホール化によってEメールが紛失する場合があることに注意してください。
- **確認されたスパムへの対策(Confirmed Spam Action)**: ここでは、スパムと確認されたメッセージに対する対策を定義できます。

これら2種類のスパムに対する処理を、さまざまな対策から選択できます。

- **オフ(Off)**: メッセージはスパムとしてマークされたり、フィルタされません。
- **警告(Warn)**: メッセージはフィルタされません。その代わりに、スパムフラグがメッセージヘッダに追加され、スパムマーカがメッセージの件名に追加されます。
- **隔離(Quarantine)**: メッセージはブロックされ、Eメールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。

スパムマーカ(Spam Marker): このオプションで、スパムマーカを指定できます。スパムマーカとは、スパムメッセージをすばやく簡単に識別できるように、メッセージの件名行に追加される文字列です。デフォルトでは、スパムメッセージを示すために`*SPAM*`という文字列が使用されます。

表現フィルタ(Expression Filter): 表現フィルタは、特定の表現を探してメッセージの件名や本文をスキャンします。ここにリストされた表現を含むEメールはブロックされます。ただし、*【メールセキュリティ(Mail Security)】*>>*【POP3】*>>*【詳細(Advanced)】*タブでプリフェッチオプションが有効になっている場合は、Eメールは隔離場所に送られます。表現は*Perl互換の正規表現*で指定できます。たとえば、「online dating」などの簡単な文字列は、大文字と小文字を区別しないで解釈されます。

設定を保存するには*【適用(Apply)】*をクリックします。

送信者ブラックリスト(Sender Blacklist)

受信するPOP3セッションのエンベロープの送信者が、このブラックリストのアドレスと照合されます。エンベロープの送信者がブラックリストにある場合、メッセージは隔離され、件名行に*Other*とマークされます。
ブラックリストに新しいアドレスパターンを追加するには、*【ブラックリストアドレスパターン(Blacklisted Address Pattern)】*ボックスでプラスアイコンをクリックし、アドレス(の一部)を入力してから、*【適用(Apply)】*をクリックします。ワイルドカードとしてアスタリスク(*)を使用できます(例: `*@abbeybnknational.com`)。

10.3.4除外

【POP3】>>*【除外(Exceptions)】*タブで、さまざまなセキュリティ機能から除外するクライアントホスト/ネットワークや送信者アドレスを定義できます。

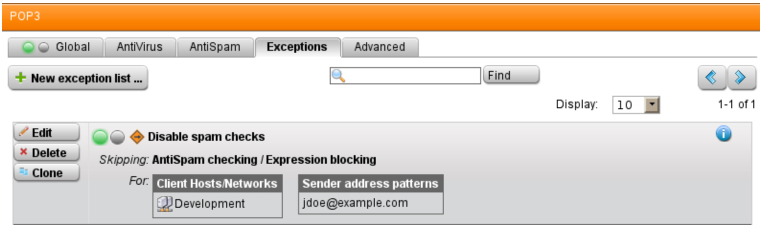


図107 POP3プロキシ(POP3 Proxy):除外リスト

除外ルールを作成するには、次の手順に従います。

1. **【除外(Exception)】タブで、【新規除外リスト(New Exception List)】をクリックします。**
   *【除外リストを作成(Create Exception List)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): この除外を説明する名前を入力します。

   スキップするチェック(Skip These Checks): スキップするセキュリティチェックを選択します。詳細は、*「メールセキュリティ」>>「SMTP」>>「アンチウイルス」*および*「アンチスパム」*を参照してください。

   スキップするクライアントホスト/ネットワーク(For These Client Hosts/Networks): セキュリティチェックをスキップする送信元ホスト/ネットワーク(メッセージを発信したホストまたはネットワーク)を選択します。

   > **注 -** ローカルメッセージはデフォルトでスキャンされないので、ローカルホストには除外を作成する必要はありません。

   このオプションを選択すると、*【ホスト/ネットワーク(Hosts/Networks)】*ダイアログボックスが開きます。「+」記号またはフォルダ記号をクリックして、ホストあるいはネットワークを追加できます。

   送信者アドレスで除外(These Sender Addresses): 定義したセキュリティチェックをスキップする送信者のEメールアドレスを選択します。
   このオプションを選択すると、*【送信者(Senders)】*ダイアログボックスが開きます。完全で有効なEメールアドレスを入力するか(例:`jdoe@example.com`)、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのEメールアドレスを指定できます(例:`*@example.com`)。

> **注 -** 送信者アドレスは容易に偽造できるため、【*送信者(Senders)*】オプションを使用する際は注意が必要です。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   新しい除外が【*除外(Exceptions)*】リストに表示されます。

例外を編集または削除するには、対応するボタンをクリックします。

10.3.5詳細

【*POP3*】>>【*詳細(Advanced)*】タブで、POP3 プロキシの基本的な設定を構成できます。さらに、このタブには、POP3プロキシのプリフェッチオプションが含まれています。プリフェッチオプションにより、POP3サーバからメッセージをプリフェッチしてデータベースに保存できます。

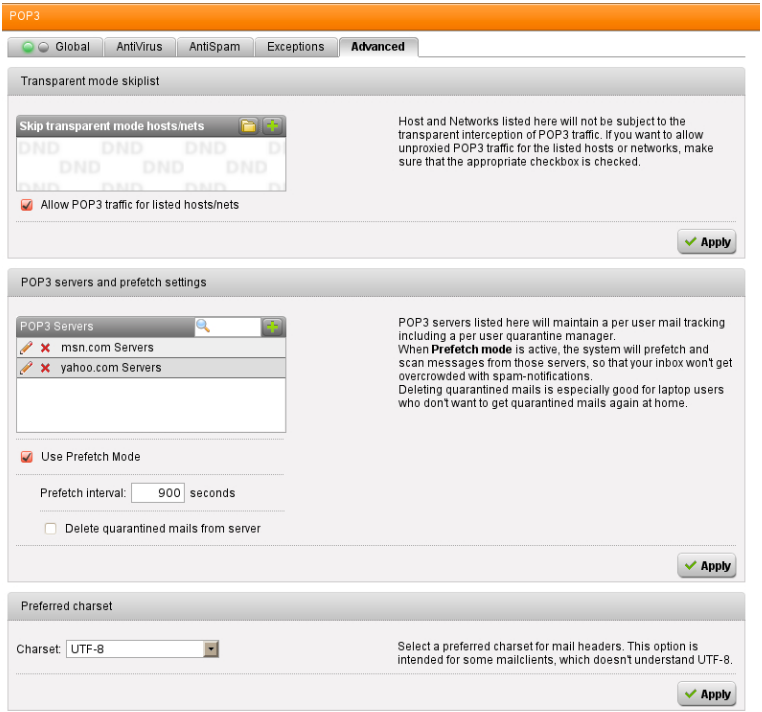


図108 POP3プロキシ(POP3 Proxy):詳細設定

透過モードスキップリスト(Transparent Mode Skiplist)

このオプションは、POP3プロキシを透過モードで実行している場合のみ有用です。*【透過モード時にスキップするホスト/ネット(Skip Transparent Mode Hosts/Nets)】*ボックスにリストされているホストとネットワークは、POP3トラフィックの透過的インターセプションの対象とはなりません。ただし、これらのホストおよびネットワークでPOP3トラフィックを許可するには、*【リスト内のホスト/ネットワークのPOP3トラフィックを許可(Allow POP3 Traffic For Listed Hosts/Nets)】*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

POP3サーバとプリフェッチ設定(POP3 Servers And Prefetch Settings)

プロキシが認識するために、ここに1つ以上のPOP3サーバを入力します。さらに、プリフェッチをオンにできます。

POP3サーバ(POP3 Servers): お客様のネットワークまたはエンドユーザが使用するPOP3サーバを指定します。
POP3サーバを指定しない場合にプロキシがメールを確認すると、プロキシは同じ接続でそのメールの代わりに、Eメールを隔離したことを受信者に通知するメッセージをただちに送ります。隔離されたメールは【*メールマネージャ(Mail Manager)*】で表示できますが、サーバやアカウントに関連付けられていないため、後の接続でリリースする(取り出して再配信する)ことはできません。一般的には、隔離されたEメールのリリースは、プリフェッチされたメッセージのみで有効です。

以下の2つのシナリオがあります。

- POP3サーバを指定してプリフェッチを無効にした場合、プロキシは、隔離されたEメールがどのサーバ/アカウントに属するかを追跡します。したがって、隔離されたEメールは、クライアントがメールボックスを次回ポーリングしたときにリリースできます。これが機能するには、プロキシは、どのIPアドレスがどのサーバに属するかを(お客様がメールクライアントで入力したFQDNによって)確実に特定する必要があります。

- POP3サーバを指定してプリフェッチを有効にした場合、POP3プロキシは新しいメッセージがないかどうかPOP3サーバを定期的に確認します。新しいメッセージが届いている場合、それはPOP3プロキシにコピーされ、スキャンされて、ASGのデータベースに保存されます。メッセージはPOP3サーバに留まります。クライアントは新しいメッセージをフェッチする(取り出す)とき、POP3プロキシと通信して、このデータベースからメッセージを取り出します。

プリフェッチをサポートしているPOP3プロキシには、以下のようなさまざまなメリットがあります。

- クライアントとプロキシ(またはその逆)のタイムアウトの問題はありません。
- Eメールを事前にスキャンするため、メッセージははるかに迅速に配信されます。
- ブロックされたメッセージはユーザポータルからリリースでき、次のフェッチに含まれます。

メッセージが悪意のコンテンツを含んでいたためにブロックされた場合、またはスパムと特定されたためにブロックされた場合は、クライアントには配信されません。それらのメッセージは隔離されます。隔離されたメッセージはユーザポータルの【*メールマネージャ(Mail Manager)*】セクションに保存され、そこで削除またはリリースされます。

プリフェッチモードを使用(Use Prefetch Mode): プリフェッチモードを有効にするには、このチェックボックスを選択して、1つ以上のPOP3サーバを【*POP3サーバ(POP3 Server)*】ボックスに追加します。

プリフェッチ間隔(Prefetch Interval): POP3プロキシがPOP3サーバに接触してメッセージをプリフェッチする時間間隔を選択します。

注 - メールクライアントがPOP3サーバへの接続を許可される間隔は、サーバごとに異なります。したがって、プリフェッチ間隔は、POP3サーバで許可されている間隔より短く設定しないようにしてください。この理由は、POP3サーバへのアクセスがブロックされると、POP3メッセージのダウンロードは失敗に終わるからです。
また、複数のメールクライアントが同じPOP3アカウントをクエリする場合があることにも注意してください。POP3サーバからメッセージがフェッチされると、次回サーバにアクセスできるようになるまでタイマーが再始動します。このためにPOP3プロキシがPOP3サーバに4回連続してアクセスできないと(デフォルトでは15分ごとにアクセスを試行します)、アカウントのパスワードがプロキシのメールデータベースから削除され、メールクライアントがPOP3サーバにパスワードを再度送ってログインしない限り、メールはフェッチされなくなります。

隔離メールをサーバから削除(Delete Quarantined Mails From Server): このオプションを選択すると、隔離されたメッセージはPOP3サーバから即座に削除されます。これは、ユーザがASG経由ではなく、たとえば、POP3サーバのWebポータル経由でPOP3サーバに接続した場合に、スパムやウイルスメッセージの受け取りを防ぐのに役立ちます。

メッセージを取り出した後にサーバからメッセージを削除するようにEメールクライアントが設定されている場合、この情報はデータベースにも保存されます。プロキシは、次回このPOP3アカウントのメッセージをプリフェッチするときに、サーバーからそれらのメッセージを削除します。これは、クライアントがAstaro Security Gatewayからメッセージをフェッチせず、かつ、削除コマンドが設定されていない限り、メッセージはPOP3サーバから削除されないことを意味します。したがって、それらはまだ、たとえばEメールプロバイダーのWebポータルで読むことができます。
以下の場合、隔離されたメッセージはPOP3サーバから削除されます。

- メッセージをメールマネージャで手動で削除した場合。
- ユーザがユーザポータルでメッセージを手動で削除した場合。
- メッセージが(隔離レポートまたはユーザポータルのいずれかを介して)リリースされ、配信時にメッセージを削除するようにユーザのEメールクライアントが設定されている場合。
- 通知メッセージが削除された場合。
- 保存期間が過ぎた場合(「メールマネージャ」の章の「設定」のセクションを参照してください)。

ただし、プリフェッチモードでは、隔離されたスパムメッセージは、クライアントコマンドではPOP3サーバから直接削除できません。

注 - プリフェッチ機能が正常に機能するためには、Eメールクライアントは少なくとも1回はPOP3サーバに接続する必要があります。これは、このユーザのためにPOP3メッセージをフェッチするには、Astaro Security Gateway は、POP3サーバ名、ユーザ名、およびユーザのパスワードをデータベースに保存する必要があるからです。ただし、これは、Astaroユーザポータル(詳細は「ユーザポータル」を参照)でPOP3アカウント資格情報を設定しても、アーカイブで*きません*。プリフェッチされたメッセージをこのユーザのポータルと毎日の隔離レポートに表示するには、ユーザポータルでPOP3アカウント資格情報が必要です。

SSL は現在サポートされていません。したがって、SSLアクセスのみ提供しているメールプロバイダーのメール(googlemailなど)は、プロキシでフィルタできません。

fetchmailユーザへの注記:セキュリティ上の理由から、メールサーバからのEメールのダウンロードに`TOP`メソッドはサポートされていません。したがって、`TOP`によって受信したメッセージはスキャンできません。ただし、`fetchall`オプション(コマンドラインの `-a`)を指定するとスキャンできます。詳細は、fetchmailのマニュアルの「RETRまたはTOP」を参照してください。

優先文字コード(Preferred Charset)

このセクションでは、メールヘッダは、何らかの方法でASGによって変更された(例:BATV)メールヘッダで今後使用するUTF-8以外の文字コードを選択できます。この機能は、UTF-8を理解しないメールクライアントをユーザが使用している場合に便利です。一般に、メールヘッダのデフォルトの文字セットはすべての地域で問題なく機能します。したがって、この設定を変更するのは、これが絶対に必要であると確信している場合のみにしてください。不明な場合は、デフォルトの*UTF-8*を維持してください。

10.4暗号化

Eメールが個人的な目的やビジネス目的で使用する主な電子通信手段となって以来、プライバシーや認証に関する懸念が高まっています。Eメールは平文形式で伝送されますが、これを一般的に言うと、ハガキと同じようにすべての人が読めるということです。さらに、身元を偽るのが容易であるため、送信者が本当に本人であるかどうかを受信者が見分けられることは重要です。

通常、これらの問題はEメールの暗号化とデジタル署名で解決できます。これにより、Eメールメッセージは電子的に署名され、暗号によって符号化されます。この結果、Eメールを開いてコンテンツを閲覧できるのはメッセージ受信者のみとなり(プライバシー)、送信者の身元が確認されるようになります(認証)。つまり、このプロセスでは「ハガキの電子版」を送付するという考えが否定され、書留郵便や配達証明郵便に近いプロセスとなります。

最先端の暗号技術では、対称と非対称という2種類のメール暗号化方式があります。いずれも標準的な方式となっており、さまざまなアプリケーションで利用されています。対称鍵暗号とは、送信者と受信者が同じ鍵を共有する暗号化方式です。

一方、非対称鍵暗号(あるいは公開鍵暗号)とは、各ユーザが2つの暗号鍵(データを暗号化する公開鍵と復号化のための秘密鍵(プライベート鍵))を持つ暗号方式です。公開鍵は自由に公開されますが、秘密鍵はユーザが厳重に保管します。

対称暗号方式の欠点として、送信者と受信者が安全に通信するためには、両者があらかじめ鍵を決め、これを互いだけの秘密として維持する必要があります。両者が離れた場所にいる場合、送信中に秘密鍵が開示されないようにしなければなりません。そのため、対称暗号方式では、鍵の受け渡しに関する問題が常に存在します。つまり、「他者に傍受されることなく受信者に鍵を伝えるにはどうすればいいか」という問題です。公開鍵暗号方式は、この問題に対処するために開発されました。公開鍵暗号方式では、ユーザは安全ではないチャネル上でも安全に通信することができ、あらかじめ共有鍵を決める必要はありません。

Eメール暗号化の必要性から、多種多様な公開鍵暗号化標準が生まれました。最も有名なのはS/MIMEとOpenPGPであり、Astaro Security Gatewayはその両方に対応しています。S/MIME(*Secure Multipurpose Internet Mail Extensions*)とは非対称暗号方式の標準であり、Eメール署名をMIMEにカプセル化します。通常、S/MIMEは公開鍵基盤(PKI)内で使用され、デジタル証明の階層構造に基づいており、信頼できるインスタンスとして認証局(CA)を必要とします。CAは、電子鍵のペアを身元情報とバインドして電子証明書を発行します。電子証明書は、パスポートなど従来からある身分証明書の電子版と考えることができます。技術的に言うと、CAは特定のX.500*識別名(DN)*またはEメールアドレスなどの*別名*に公開鍵をバインドして証明書を発行します。

デジタル証明書により、任意の鍵を使用する権利を主張する人にその権利があるかどうかを確認することができます。これは、ある人がCAを信頼しており、公開鍵がこのCAによって署名されていることを確認できるのであれば、この人はこの公開鍵が本当に所有者と主張する人のものであると安心できる、という考え方です。

一方、OpenPGP(*Pretty Good Privacy*)は、一般にWOT(*web of trust*)で採用されている非対称暗号方式を使用します。つまり、公開鍵は他のユーザによってデジタル署名され、署名するユーザは署名という行為によって、公開鍵とその人の関連性を保証します。

注 - S/MIMEとOpenPGPは類似のサービスを提供しますが、形式は大きく異なります。そのため、一方のプロトコルのユーザは、他方のプロトコルのユーザと通信できません。さらに、認証証明書を共有することもできません。

Eメール暗号化は、ユーザに対して完全に透過的です。つまり、クライアント側で追加の暗号化ソフトウェアを用意する必要はありません。一般に暗号化では、送信先の証明書または公開鍵が手元にある必要があります。受信メッセージと送信メッセージに対し、Eメール暗号化機能は次のように機能します。

- デフォルトで、内部ユーザが送信したメッセージはスキャンされ、自動的に署名され、受信者の証明書(S/MIME)または公開鍵(OpenPGP)で暗号化されます(受信者のS/MIME証明書またはOpenPGP公開鍵がASG上にある場合)。
- ASGがS/MIME証明書またはOpenPGP公開鍵を認識している外部ユーザから送られてきた暗号化済み受信メッセージは、自動的に復号化され、悪質なコンテンツが含まれないかスキャンされます。メッセージの復号化のためには、内部ユーザのS/MIME鍵またはOpenPGP秘密鍵がASGに存在している必要があります。
- ASGが認識できない外部ユーザから送られてきたか、セキュリティシステムが認識できない内部ユーザ向けの暗号化済み受信メッセージは、配達されるものの復号化はできません。従って、ウイルスやスパムのスキャンは行われません。個人用ファイアウォールなどでそのEメールにマルウェアが含まれていないことを確認するのは、受信者(内部ユーザ)の責任となります。
- クライアント側ですでに暗号化されている送信メッセージは、受信者のS/MIME証明書またはOpenPGP公開鍵が不明な場合、受信者に直接送信されます。一方、受信者のS/MIME証明書またはOpenPGP公開鍵がわかる場合、メッセージは2回暗号化されます。あらかじめ暗号化されたメッセージに悪質なコンテンツが含まれないかスキャンすることはできません。
- 復号化が可能なのは受信メールのみです。ここで「受信」と見なされるためには、送信者のEメールアドレスのドメイン名がSMTPプロファイルの一部ではないことが条件です。たとえば、`jdoe@example.com`から送信されたメッセージを復号化するためには、`example.com`というドメインがルーティング設定またはSMTPプロファイルのいずれにも設定されていないことが求められます。
- 署名/暗号化結果の概要は、各Eメールの件名行に記述されます。たとえば、あるEメールが正しく署名され、S/MIMEで暗号化されると、「S/MIME: 署名済み、暗号化済み(Signed and encrypted)」というテキストが件名の行に付加されます。

注 -Eメールクライアント(例: Microsoft OutlookまたはMozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、アンチウイルスチェックフッタオプションを無効にしてください。ただし、Eメール通信のプライバシや認証を保ちながら一般的なアンチウイルスチェックフッタを使用したい場合は、Astaro Security Gatewayの組み込みEメール暗号化機能を使用

してください。ゲートウェイ上でのEメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

10.4.1グローバル

*【メールセキュリティ(Mail Security)】>>【暗号化(Encryption)】>>【グローバル(Global)】*タブでは、Eメール暗号化機能の基本設定を定義することができます。

クロスリファレンス - Eメール暗号化の使用方法に関する総合的な説明は、Astaroナレッジベースにある『Eメール暗号化ガイド(E-Mail Encryption Guide)』をご確認ください(*「ASGバージョン7」>>「Astaroマニュアルおよびガイド」*の順にアクセスします)。

注 - 暗号化はSMTPのみで機能し、POP3では機能しません。

Eメール暗号化を使用するためには、CA証明書とCA鍵から成る*認証局*(CA)を作成しておく必要があります。CA証明書はダウンロードしてローカルに保存することができます。さらに、図で示すように、他のユニットに外部CA(S/MIME認証局)としてインストールし、2つのAstaro Security Gatewayユニット間で透過的なEメール暗号化を実現することもできます。

注 -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの*【インターネットオプション】>>【セキュリティ】*で設定します。さらに、Internet Explorer 7を使用する場合は、*【信頼済みサイトゾーン】*で*【ファイルのダウンロード時に自動的にダイアログを表示】*を選択します。

図109 メール暗号化(E-mail Encryption):2つのAstaro Security Gateway ユニットの使用

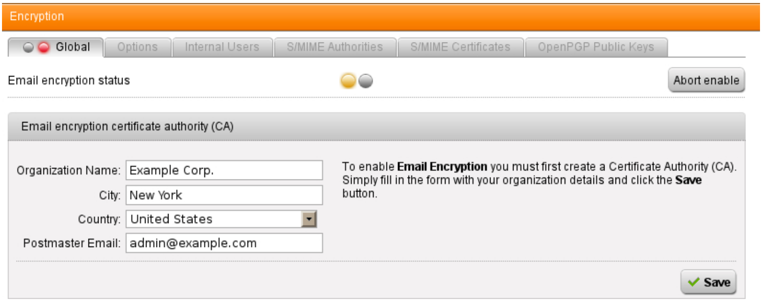


図110 メール暗号化(E-mail Encryption):Eメール暗号化の有効化

Eメール暗号化を設定するには、次の手順に従ってください。

1. ***【グローバル(Global)】タブで、Eメール暗号化を有効化します。***
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【Eメール暗号化認証局(CA)(E-mail Encryption Certificate Authority(CA))】*エリアが編集可能になります。

2. **認証局(CA)を作成します。**
   *【Eメール暗号化認証局(CA)(E-mail Encryption Certificate Authority(CA))】*エリアのフォームに記入します。デフォルトで、このフォームには*【マネジメント(Management)】>>【システム設定(System Settings)】>>【組織(Organizational)】*タブの値が入力されています。

3. ***【保存(Save)】*をクリックします。**
   ステータスアイコンが緑色になり、次の証明書と鍵が作成されます。

   - S/MIME CA証明書
   - OpenPGP ポストマスタ鍵

   これが完了するまで数分かかる可能性があります。S/MIME CA証明書またはOpenPGPポストマスタ鍵のフィンガープリントが表示されない場合、WebAdminの右上隅にある*【リロード(Reload)】*ボタンをクリックしてください。証明書と鍵は、ダウンロードしてローカルに保存できます。

*【Eメール暗号化(E-mail Encryption)】*メニューのすべての設定を工場出荷時のデフォルト設定にリセットするには、*【Eメール暗号化システムを今すぐリセット(Reset E-mail Encryption System Now)】*ボタンを使用します。

10.4.2オプション

*【暗号化(Encryption)】>>【オプション(Options)】*タブでは、Astaro Security Gatewayの公開鍵暗号フレームワーク内で使用されるデフォルトポリシを定義できます。

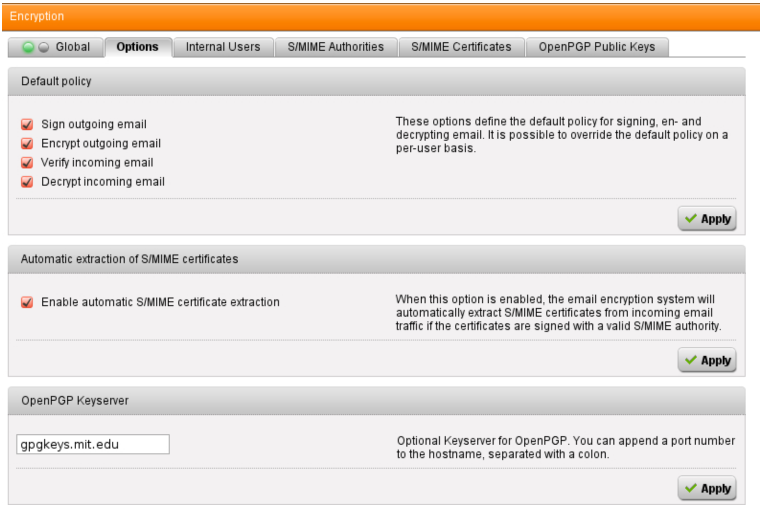


図111 メール暗号化(E-mail Encryption):オプション

デフォルトポリシ(Default Policy): Eメールの暗号化に関するデフォルトポリシを指定します。これらの設定は、カスタマイズされた設定で上書きできます。

次の作業を実行できます。

- 送信Eメールへの署名
- 送信Eメールの暗号化
- 受信Eメールの検証
- 受信Eメールの復号化

設定を保存するには*【適用(Apply)】*をクリックします。

注 - 暗号化が機能するためには、送信者が【内部ユーザ(Internal Users)】リストに含まれている必要があります。S/MIME証明書またはOpenPGP公開鍵がゲートウェイに存在する受信者に向けた送信Eメールは、デフォルトで暗号化されます。これらの受信者に対する暗号化

を無効にするには、当該受信者のS/MIME証明書またはOpenPGP公開鍵を削除してください。証明書または公開鍵がASGに不明の場合、Eメールは暗号化されずに送信されます。

S/MIME証明書の自動抽出(Automatic Extraction of S/MIME Certificates)

このオプションを選択すると、S/MIME証明書は受信Eメールから自動的に抽出されます。このとき、そのEメールに添付された証明書が、信頼される認証局に署名されていることが条件となります。信頼される認証局とは、*【メールセキュリティ(Mail Security)】>>【暗号化(Encryption)】>>【S/MIME認証局(S/MIME Authorities)】*タブに表示される、ユニットにあるCAです。さらに、証明書の自動抽出が機能するためには、Astaro Security Gatewayの時間と日付が、証明書の有効期間内である必要があります。証明書の抽出が成功すると、証明書は*【メールセキュリティ(Mail Security)】>>【暗号化(Encryption)】>>【S/MIME証明書(S/MIME Certificates)】*タブに追加されます。これが完了するまで5～10分かかる可能性があります。設定を保存するには*【適用(Apply)】*をクリックします。

OpenPGP鍵サーバ(OpenPGP Keyserver)

OpenPGP鍵サーバは公開PGP鍵をホストします。ここで、OpenPGP鍵サーバを追加することができます。暗号化された受信Eメールや暗号化する送信Eメールで、該当する公開鍵がASGに不明の場合、ASGは所与のサーバから公開鍵を取得しようとします。

10.4.3内部ユーザ

メッセージの署名と復号化を行うためには、S/MIME鍵またはOpenPGP秘密鍵がASGに存在している必要があります。*【暗号化(Encryption)】>>【内部ユーザ(Internal Users)】*タブでは、Eメール暗号化を有効にするユーザに対して、個別のS/MIME鍵/証明書またはOpenPGP鍵ペア(あるいはその両方)を作成できます。

図112 メール暗号化(E-mail Encryption):内部ユーザのリスト

内部Eメールユーザを作成するには、次の手順に従います。

1. **【内部ユーザ(Internal Users)】タブで【新規Eメール暗号化ユーザ(New Email Encryption User)】をクリックします。**
   *【新規ユーザの作成(Create New User)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   Eメールアドレス(E-mail Address): ユーザのEメールアドレスを入力します。

   フルネーム(Full Name): ユーザの名前を入力します。

   署名(Signing): 次の署名オプションを使用できます。

   - デフォルトポリシの使用(Use Default Policy):*【オプション(Options)】*タブのポリシが使用されます。
   - オン(On):Eメールは、ユーザの証明書を使用して署名されます。
   - オフ(Off):Eメールは署名されません。

   暗号化(Encryption): 次の暗号化オプションを使用できます。

   - デフォルトポリシの使用(Use Default Policy):*【オプション(Options)】*タブのポリシが使用されます。
   - オン(On):Eメールは、受信者の公開鍵を使用して暗号化されます。
   - オフ(Off):Eメールは暗号化されません。

   検証(Verifying): 次の検証オプションを使用できます。

   - デフォルトポリシの使用(Use Default Policy):*【オプション(Options)】*タブのポリシが使用されます。
   - オン(On):Eメールは、送信者の公開鍵を使用して検証されます。
   - オフ(Off):Eメールは検証されません。

   復号化(Decryption): 次の複合化オプションを使用できます。

   - デフォルトポリシの使用(Use Default Policy):*【オプション(Options)】*タブのポリシが使用されます。
   - オン(On):Eメールは、ユーザの証明書を使用して復号化されます。
   - オフ(Off):Eメールは復号化されません。

   S/MIME: S/MIME証明書と鍵をシステムに自動生成させるか、証明書を`PKCS#12`形式でアップロードするかを選択します。証明書をアップロードする場合、`PKCS#12`ファイルの保護に使用されたパスフレーズを知っている必要があります。`PKCS#12`ファイルに

は、S/MIME鍵と証明書の両方が含まれていなければなりません。このPKCS#12ファイルに含まれているすべてのCA証明書は無視されます。

OpenPGP: 秘密鍵と公開鍵から成るOpenPGP鍵ペアをシステムに自動生成させるか、鍵ペアをASCII形式でアップロードするかを選択します。秘密鍵と公開鍵の両方が1つのファイルに格納されており、ファイルにパスフレーズが含まれていないことが必要です。

> **注 -** あるユーザに対してS/MIMEとOpenPGPの両方が設定されている場合、このユーザから送信されるEメールの署名と暗号化はS/MIMEを使用して行われます。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
新しいユーザが【*内部ユーザ(Internal Users)*】リストに表示されます。

ステータスアイコンを使用して、いずれかの鍵(または両方)の使用をオフにします。鍵を削除する必要はありません。

> **注 -** セキュリティ上の理由から、ダウンロード用に提供されたそれぞれのファイルにはS/MIME証明書とOpenPGP公開鍵のいずれかのみが含まれています。S/MIME鍵とOpenPGP秘密鍵はシステムからダウンロードできません。Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (https://192.168.2.100など)を信頼されるサイトに追加します。これはIEの【*インターネットオプション*】>>【*セキュリティ*】で設定します。さらに、Internet Explorer 7を使用する場合は、【*信頼済みサイトゾーン*】で【*ファイルのダウンロード時に自動的にダイアログを表示*】を選択します。

10.4.4S/MIME認証局

【*暗号化(Encryption)*】>>【*S/MIME認証局(S/MIME Authorities)*】タブで、信頼する外部*認証局*(CA)の証明書(つまり公開鍵)をインポートします。これにより、このCAが証明書に署名したすべての受信Eメールについても信頼することになります。【*メールセキュリティ(Mail Security)*】>>【*暗号化(Encryption)*】>>【*オプション(Options)*】タブで【*S/MIME証明書の自動抽出(Automatic Extraction of S/MIME Certificates)*】オプションを選択した場合、ここにリストされたCAによって署名された証明書が自動的に抽出され、【*メールセキュリティ(Mail Security)*】>>【*暗号化(Encryption)*】>>【*S/MIME証明書(S/MIME Certificates)*】タブに配置されます。

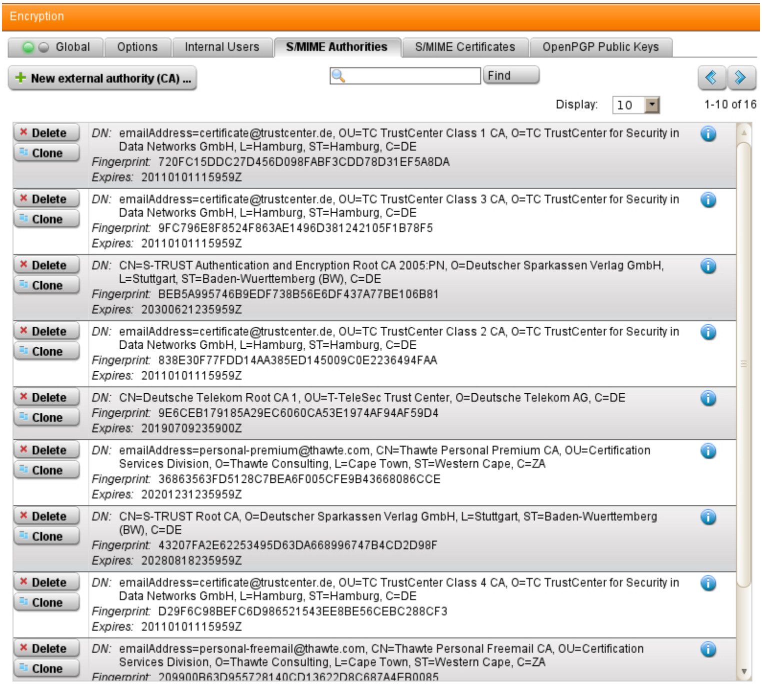


図113 メール暗号化(E-mail Encryption):S/MIME認証局のリスト

外部S/MIME認証局をインポートするには、次の手順に従います。

1. ***【S/MIME認証局(S/MIME Authorities)】タブで【新規外部認証局(CA)(New External Authority(CA))】をクリックします。***
   *【外部認証局の追加(Add External Authority)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   形式(Format): CAの形式を選択します。次の形式を選択できます。

   - der(バイナリ)
   - pem(ASCII)

> **注 -** Microsoft Windowsオペレーティングシステムでは、der形式とpem形式の両方に対してファイル拡張子cerを使用します。そのため、アップロードする証明書をバイナリ形

式にするかASCII形式にするかを、あらかじめ決定しておく必要があります。次に、これに従ってドロップダウンリストで形式を選択します。

証明書(Certificate): フォルダアイコンをクリックして、【*ファイルのアップロード(Upload File)*】ダイアログボックスを開きます。ファイルを選択して【*保存(Save)*】をクリックします。

コメント(Comment)(オプション) : 説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   CAが【*S/MIME認証局(S/MIME Authorities)*】リストに表示されます。

Astaro Security Gateway の出荷時には、商用CAの各種公開鍵があらかじめインストールされています。これにより、これらのCAに基づいてPKIを管理しているコミュニケーションパートナーとお客様の間で、Eメールの暗号化が促進されます。次のリンクは、有名なルート証明書のURLです。

- Trustcenter
- S-TRUST
- Thawte
- VeriSign
- GeoTrust

さらに、他のAstaro Security Gatewayユニットのインストールすると、2つのAstaro Security Gatewayユニット間でEメールを透過的に暗号化することができます。

10.4.5S/MIME証明書

【*暗号化(Encryption)*】>>【*S/MIME証明書(S/MIME Certificates)*】タブでは、外部S/MIME証明書をインポートすることができます。証明書がここにリストされている受信者へのEメールは自動的に暗号化されます。特定の受信者に対する暗号化を無効にするには、リストから証明書を削除してください。

注 - S/MIME証明書を手動でアップロードすると、証明書に記載された人を識別できるCA証明書がなくても、証明書に関連付けられたEメールアドレスからのメッセージが常に信頼されるようになります。つまり、S/MIME証明書を手動アップロードするということは、送信元に「信頼できる」というラベルを貼り付けるということになります。

図114 メール暗号化(E-mail Encryption):S/MIME証明書のリスト

外部S/MIME証明書をインポートするには、次の手順に従います。

1. ***【S/MIME証明書(S/MIME Certificates)】タブで【新規外部S/MIME証明書(New External S/MIME Certificate)】をクリックします。***
   *【S/MIME証明書の追加(Add S/MIME Certificate)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   形式(Format): 証明書の形式を選択します。次の形式を選択できます。

   - pem(ASCII)
   - der(バイナリ)

   注 - Microsoft Windowsオペレーティングシステムでは、der形式とpem形式の両方に対してファイル拡張子cerを使用します。そのため、アップロードする証明書をバイナリ形式にするかASCII形式にするかを、あらかじめ決定しておく必要があります。次に、これに従ってドロップダウンリストで形式を選択します。

   証明書(Certificate): フォルダアイコンをクリックして、*【ファイルのアップロード(Upload File)】*ダイアログボックスを開きます。ファイルを選択して*【保存(Save)】*をクリックします。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   新しいS/MIME証明書が*【S/MIME証明書(S/MIME Certificates)】*リストに表示されます。

10.4.6OpenPGP公開鍵

*【暗号化(Encryption)】>>【OpenPGP公開鍵(OpenPGP Public Keys)】*タブでは、OpenPGP公開鍵をインストールすることができます。.asc形式のファイルを提供する必要があります。キーリング全体のアップロードがサポートされています。

注 - パスフレーズで保護されているキーリングはアップロードしないでください。

このキーリングに含まれるすべての公開鍵がインポートされ、メッセージの暗号化に使用できるようになります。公開鍵がここにリストされている受信者へのEメールは自動的に暗号化されます。特定の受信者に対する暗号化を無効にするには、リストから公開鍵を削除してください。

注 - 鍵ごとに1つのEメールアドレスだけがサポートされます。1つの鍵に複数のアドレスが関連付けられている場合、「最初の」アドレスのみが使用されます(この順序は、OpenPGPでのアドレスのソート方法に応じています)。インポートしたい鍵に複数のアドレスが関連付けられている場合、その鍵をにインポートする前に、OpenPGPまたはその他のツールで不要なアドレスを削除する必要があります。Astaro Security Gateway.

図115 メール暗号化(E-mail Encryption):OpenPGP公開鍵のリスト

OpenPGP公開鍵をインポートするには、次の手順に従います。

1. ***【OpenPGP公開鍵(OpenPGP Public Keys)】タブで、【キーリングファイルのインポート(Import Keyring File)】をクリックします。***
   *【OpenPGPキーリングファイルのインポート(Import OpenPGP Keyring File)】*ダイアログボックスが開きます。

2. **OpenPGP鍵をアップロードします。**
   フォルダアイコンをクリックして、*【ファイルのアップロード(Upload file)】*ダイアログボックスを開きます。ファイルを選択して*【保存(Save)】*をクリックします。

   鍵または鍵のリスト(ファイルに複数の鍵が含まれている場合)が表示されます。

3. **鍵を1つ以上選択し、*【選択した鍵をインポート(Import Selected Keys)】*をクリックします。**
   鍵が*【OpenPGP公開鍵(OpenPGP Public Keys)】*リストに表示されます。

注 - 鍵にはEメールアドレスが1つ関連付けられていなければならず、関連付けられていない場合、インストールは失敗します。

10.5隔離レポート

Astaro Security Gateway は、さまざまな理由からブロックされて隔離場所にリダイレクトされたすべてのメッセージSMTP およびPOP3)を含むEメールの隔離場所を用意しています。ここには、配信待ちのメッセージ、悪意あるソフトウェアに感染したメッセージ、疑わしい添付物を含むメッセージ、スパムと特定されたもの、または単に不要な表現を含むメッセージが含まれます。

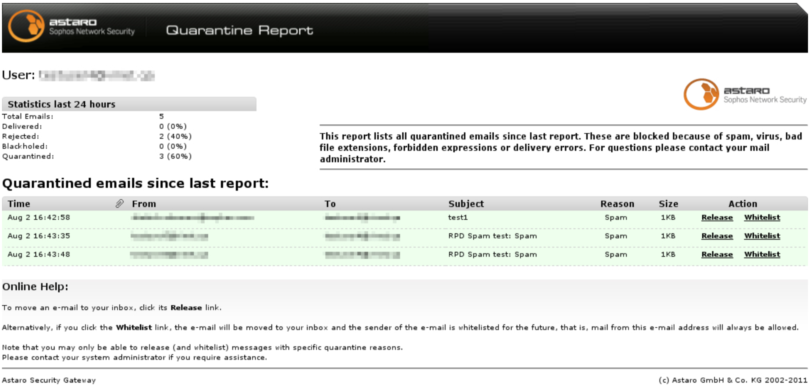


図116 当製品の隔離レポート Astaro Security Gateway

メッセージが間違って隔離されて保留されるリスク(いわゆる*誤検出*)を最小限に抑えるために、Astaro Security Gateway は、隔離されたメッセージについて報告する隔離レポートをユーザに毎日送信します。ユーザに複数のメールアドレスが設定されている場合は、それぞれのEメールアドレスに個々の隔離レポートが送信されます。ユーザポータルで追加のPOP3アカウントが設定されており、Astaro Security GatewayのPOP3プロキシがプリフェッチモード(POP3サーバからメッセージをプリフェッチし、ローカルデータベースに保存することが可能)である場合にも、これは適用されます。隔離レポートでは、ユーザはスパムエントリをクリックしてメッセージを隔離場所からリリースしたり、今後のために送信者をホワイトリストに追加できます。

隔離レポートの詳細について、以下に少し説明します。

- 隔離レポートは、EメールアドレスがSMTPプロファイルに含まれているドメインの一部であるユーザに対してのみ送信されます。隔離レポートには、*【SMTP】>>【ルーティング(Routing)】*タブの*【ドメイン(Domains)】*ボックスで指定したものや、SMTPプロファイルの*【ドメイン(Domains)】*ボックスで指定したものが含まれます。

- POP3プリフェッチオプションが無効の場合、このアカウントに送信された隔離されたメッセージは隔離レポートには表示されません。代わりに、各ユーザの受信トレイに、一般的なAstaro POP3のブロックされたメッセージが表示されます。したがって、隔離レポートまたはユーザポータルを使用してメッセージをリリースすることはできません。このようなEメールは、管理者が`zip`形式でメールマネージャからダウンロードすることでのみ配信できます。
- 隔離場所からリリースできるのは、スパムメールだけです。他の理由で隔離されたメッセージ(ウイルスや疑わしい添付ファイルを含むメッセージなど)は、当製品のメールマネージャで管理者によってのみ隔離場所からリリースできます。Astaro Security Gateway. さらに、ユーザは、現在隔離されているすべてのメッセージをAstaroユーザポータルで確認することができます。
- スパムメールに複数の受信者がいる場合は、メーリングリストの場合と同様に、受信者の誰かがそのEメールをリリースすると、メーリングリストのEメールアドレスがシステムで設定されている場合は、そのEメールはその受信者のみにリリースされます。そうでない場合は、そのEメールはすべての受信者に同時に配信されます。詳細は、【*メールセキュリティ(Mail Security)*】>>【*隔離レポート(Quarantine Report)*】>>【*除外(Exceptions)*】タブの【*内部メーリングリストの定義(Define internal mailing lists)*】オプションを参照してください。<
- 管理者は、Astaro Security Gatewayでユーザが設定されていないSMTP Eメールアドレスに送信されたEメールを、隔離レポートまたはメールマネージャからリリースできます(ホワイトリストへの追加はしない)。ただし、このユーザが設定されていないため、ユーザポータルへのアクセスはできません。
- メーリングリストに送信されたスパムメールはホワイトリストにリストできません。
- EメールクライアントでEメールのヘッダを正しくエンコードしていないと、デイリーの隔離レポートのEメールが正しく表示されない場合があります。

10.5.1グローバル

【*隔離レポート(Quarantine Report)*】>>【*グローバル(Global)*】タブで、デイリーの隔離レポートの送信時刻を定義して、隔離レポートに表示されるメッセージテキストを記述できます。

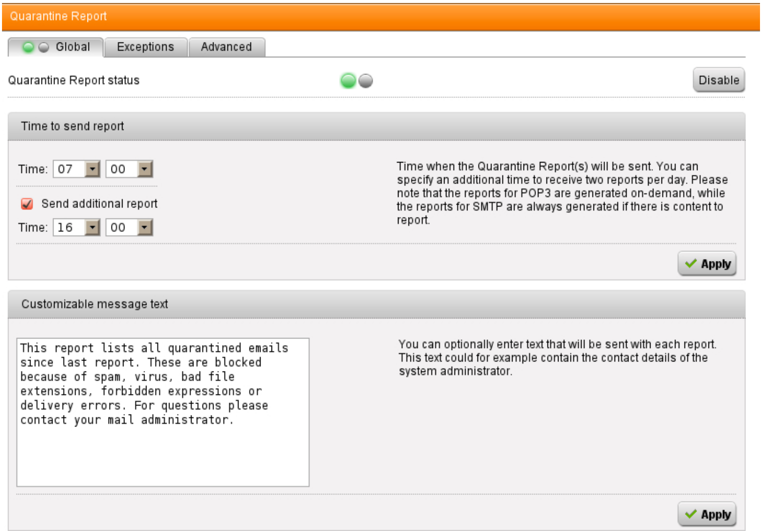


図117 隔離レポート:隔離レポートの有効化

隔離レポートの設定を編集するには、隔離レポートを有効にします。ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。
ステータスアイコンが緑色に変わります。

レポート送信時刻(Time to Send Report)

ここでデイリーの隔離レポートの送信時刻を定義できます。ドロップダウンリストで時刻を選択し、【*適用(Apply)*】をクリックします。
追加のレポートを送信することもできます。これを行うには、【*追加のレポートを送信(Send Additional Report)*】チェックボックスにチェックを入れ、時刻を設定して、【*適用(Apply)*】をクリックします。

カスタマイズ可能なメッセージテキスト(Customizable Message Text)

ここで、隔離レポートの序文となるテキストをカスタマイズできます。必要に応じてメッセージテキストを変更して、【*適用(Apply)*】をクリックします。

注 – カスタマイズ可能なメッセージテキストボックスではHTMLタグは使用できません。

注 – 家庭用ライセンスを使用している場合は、カスタマイズできません。

10.5.2除外

【隔離レポート(Quarantine Report)】>>*【除外(Exception)】*タブで、デイリーの隔離レポートの受信から除外するEメールアドレスのスキップリストを定義できます。

図118 隔離レポート：除外

隔離レポートをスキップ(Skipping Quarantine Reports)

ここで隔離通知を送信しない内部Eメールアドレスを設定できます。ここにEメールアドレスがリストされているユーザは、デイリーの隔離レポートを受信しません。完全なEメールアドレスを入力するか、または`*@example.com`のようにアスタリスク(*)をワイルドカードとして使用できます。

> **注** - スキップリストはSMTP隔離レポートにのみ適用されます。それぞれのユーザに指定されたPOP3アカウントがある場合は、POP3隔離レポートはそれにもかかわらず送信されます。

内部メーリングリストの定義(Define Internal Mailing Lists)

メーリングリストのEメールアドレスが*【メーリングリストアドレスパターン(Mailing List Address Patterns)】*ボックスで設定されている場合に(例：`newsletter@example.com`)、このメーリングリストに送信されたスパムメッセージが検知されてEメールの隔離場所にリダイレクトされたときは、このメーリングリストに含まれるすべての受信者の隔離レポートがこのスパムメッセージへのリンクを含みます。したがって、各受信者は、受信者が隔離レポートの*【リリース(Release)】*リンクをクリッ

クすると表示されるユーザプロンプトに自身のEメールアドレスを入力することで、このスパムメッセージを個々にリリースできます。

注 - メーリングリストは隔離レポートまたはユーザポータルでホワイトリスト化できません。

代わりに、特定メーリングリストのEメールアドレスを、追加Eメールアドレスとしてローカルユーザのプロファイルに入力することで、このユーザを一種のメールマネージャに設定できます。すると、このユーザの隔離レポートのみがメーリングリストに送信されたスパムメッセージへのリンクを含むようになります。【*リリース(Release)*】リンクをクリックすると、そのメーリングリストのすべての受信者に一度にスパムメッセージが送信されます。

注 - メーリングリストのEメールアドレスがユーザのプロファイルの追加Eメールアドレスとして設定されている場合は、そのメーリングリストに送信されたスパムメッセージへのリンクは、そのメーリングリストの受信者には表示されません。

ただし、メーリングリストのEメールアドレスがユーザのプロファイルおよび【*メーリングリストアドレスパターン(Mailing List Address Patterns)*】ボックスの両方で追加Eメールアドレスとして設定されている場合は、そのユーザの隔離レポートの【*リリース(Release)*】リンクからユーザプロンプトが開きます。そこでスパムメッセージの転送先のそれぞれのEメールアドレスを手動で入力して、スパムメールの受信者を決定できます。

最後に、メーリングリストのEメールアドレスがユーザプロファイルとメーリングリストアドレスパターンのどちらでも追加Eメールアドレスとして設定されていない場合は、メーリングリストに送信されたスパムメッセージは通常のEメールのように扱われます。つまり、受信者の誰かがスパムメールをリリースすると、それはメーリングリストのすべての受信者に送信されます。

要約すると、メーリングリストのEメールアドレスをメーリングリストアドレスパターンとして設定すると、隔離レポートにスパムメッセージへのリンクを持つ各ユーザは、スパムメッセージのリリース先のEメールアドレスを入力するように要求されることになります。

10.5.3詳細

【*隔離レポート(Quarantine Report)*】>>【*詳細(Advanced)*】タブで、デイリーの隔離レポートに含まれる【*リリース(Release)*】リンクに代替ホスト名とポート番号を設定できます。また、スパムメールのリリースオプションを変更することもできます。

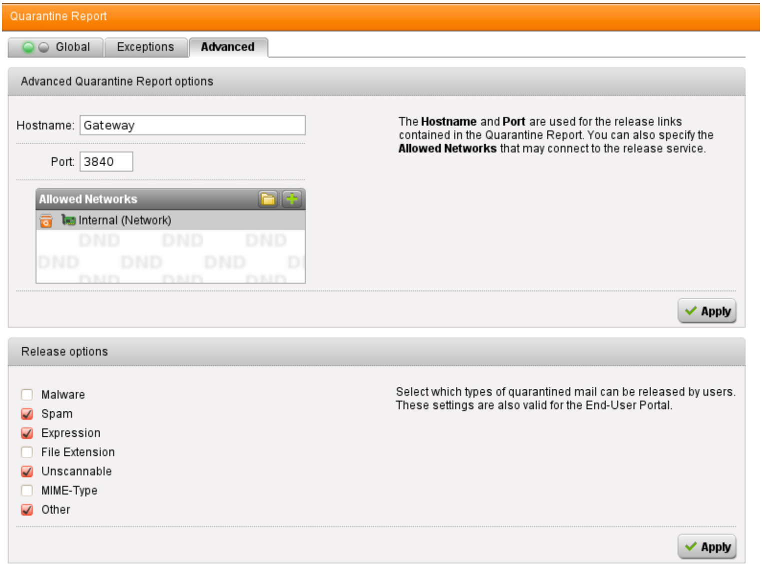


図119　隔離レポート：詳細オプション

隔離レポート詳細オプション(Advanced Quarantine Report Options)

ホスト名(Hostname)：デフォルトでは、【*マネジメント(Management)*】>>【*システム設定(System Settings)*】>>【*ホスト名(Hostname)*】タブのゲートウェイのホスト名です。ゲートウェイが送信する隔離レポートには、ハイパーリンクなどが含まれており、ユーザはこれをクリックしてEメール隔離場所からメッセージをリリースできます。デフォルトでは、これらのリンクはここで指定したホスト名をポイントしています。ユーザがインターネット上でEメールをリリースできるようにしたい場合は、パブリックに解決できる代替ホスト名をここに入力する必要があります。

ポート(Port)：デフォルトでは、ポート3840が設定されています。ポートは、1024～65535の範囲内でどの値にでも変更できます。

許可ネットワーク(Allowed Networks)：Eメールリリースサービスへの接続を許可するネットワークも指定できます。デフォルトでは、内部ネットワークのみが選択されています。

設定を保存するには【*適用(Apply)*】をクリックします。

リリースオプション(Release Options)

ここで、ユーザがリリース可能な隔離メッセージのタイプを選択できます。以下のオプションから選択できます。

- マルウェア(Malware)
- スパム(Spam)
- 表現(Expression)
- ファイル拡張子(File Extension)
- スキャン不可(Unscannable)
- MIME
- その他(Other)

設定を保存するには【*適用(Apply)*】をクリックします。

10.6メールマネージャ

メールマネージャとは、ユニットに現在保存されているすべてのEメールメッセージを管理および整理するための管理ツールです。配信待ちのメッセージや、悪意あるソフトウェアに感染している隔離メッセージ、疑わしい添付ファイルが添付されている隔離メッセージ、スパムとして識別された隔離メッセージ、または好ましくない表現が含まれている隔離メッセージなどが表示されます。メッセージをダウンロード、リリース、削除する前に、メールマネージャを使用してすべてのメッセージをレビューすることができます。メールマネージャはUTF-8に完全に対応しています。

注 -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの【*インターネットオプション*】>>【*セキュリティ*】で設定します。さらに、Internet Explorer 7を使用する場合は、【*信頼済みサイトゾーン*】で【*ファイルのダウンロード時に自動的にダイアログを表示*】を選択します。

10.6.1 メールマネージャウィンドウ

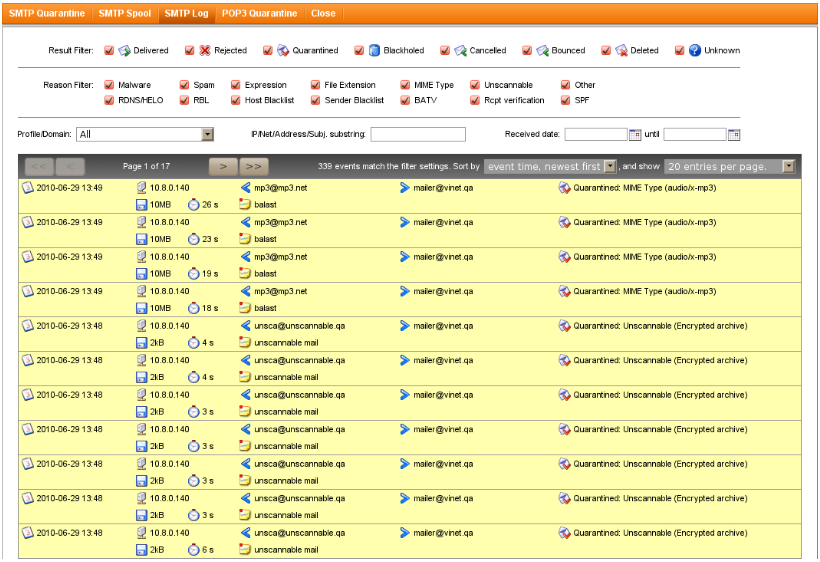


図120 メールマネージャ - Astaro Security Gateway

【メールマネージャ(Mail Manager)】ウィンドウを開くには、*【メールセキュリティ(Mail Security)】>>【メールマネージャ(Mail Manager)】>>【グローバル(Global)】タブの【新しいウィンドウでメールマネージャを開く(Open Mail Manager in New Window)】*ボタンをクリックします。メールマネージャは、次の5つのタブに分割されています。

- **SMTP隔離(SMTP Quarantine)**: 現在隔離されているすべてのメッセージを表示します。
- **SMTPスプール(SMTP Spool)**: 現在`/var/spool`にあるすべてのメッセージを表示します。これらのメッセージは、配信待ちであるか、エラーが発生したためにスプールに含まれている可能性があります。
- **SMTPログ(SMTP Log)**: SMTP経由で処理されたすべてのメッセージの配信ログを表示します。
- **POP3隔離(POP3 Quarantine)**: POP3経由でフェッチされた現在隔離されているすべてのメッセージを表示します。

- **閉じる(Close)**: これをクリックすると、【メールマネージャ(Mail Manager)】ウィンドウが閉じます。

10.6.1.1SMTP/POP3隔離

SMTPおよびPOP3隔離内のメッセージは、それぞれの隔離理由別に表示することができます。

- マルウェア(Malware)
- スパム(Spam)
- 表現(Expression)
- ファイル拡張子(File Extension)
- MIMEタイプ(SMTPのみ)
- スキャン不可(Unscannable)
- その他(Other)

チェックボックスを使用して、隔離理由を選択/選択解除します。ある理由のチェックボックスをダブルクリックすると、この理由だけが選択されます。

ヒント - メッセージを表示するには、メッセージをダブルクリックします。

プロファイル/ドメイン(Profile/Domain)(SMTP)、**アカウント(Accounts)**(POP3)あるプロファイル/ドメインまたはアカウントのメッセージのみを表示するには、プロファイル/ドメインまたはアカウントを選択します。

送信者/受信者/件名サブ文字列(Sender/Rcpt/Subject Substring): ここでは、隔離されたメッセージ内で検索する送信者、受信者、または件名を入力します。

受信日付(Received Date): 特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

ソート基準(Sort By): メッセージは、日付、件名、送信者アドレス、メッセージサイズを基準に並べ替えることができます。

表示数(And Show): 表示するエントリ数として、1ページあたり20エントリ、50エントリ、100エントリ、250エントリ、500エントリ、1000エントリ、またはすべてのメッセージを選択することができます。すべてのメッセージの表示には時間がかかる場合があります。

各メッセージの前にあるチェックボックスを使用するか、メッセージをクリックして、選択したメッセージにアクションを適用します。次の作業を実行できます。

- **ダウンロード(Download)**: 選択されたメッセージをダウンロードします。
- **削除(Delete)**: 選択されたメッセージを削除します。これを取り消すことはできません。
- **リリース(Release)**: 選択されたメッセージを隔離からリリースします。
- **リリースし、誤検出として報告(Release and Report as False Positive)**: 選択したメッセージを隔離からリリースし、スパムスキャンエンジンに誤検出として報告します。

隔離に保留されているメッセージをすべてリリースできるのは管理者だけです。Astaroユーザポータルでメッセージを確認したユーザは、明示的に許可されているメッセージのみをリリースすることができます。この権限付与設定は、*【メールセキュリティ(Mail Security)】>>【隔離レポート(Quarantine Report)】>>【詳細(Advanced)】*タブで確認できます。

グローバルクリーンアップアクションの選択(Select Global Cleanup Action): ここには、メッセージに対してグローバルに適用されるさまざまな削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

警告 - メッセージの削除を取り消すことはできません。

10.6.1.2SMTPスプール

ここには、配信待ちメッセージまたはエラーが発生したメッセージが表示されます。配信ログは、メッセージヘッダの一部でもあります。次のチェックボックスを使用して、表示するメッセージのタイプを1つだけ選択してください。

- **待機中(Waiting)**: 配信待ちのメッセージ。
- **エラー(Error)**: エラーが発生したメッセージ。あるメッセージでエラーが複数回発生した場合は、Astaroパートナーまたは Astaroサポートチームに報告してください。

ヒント - メッセージを表示するには、メッセージをダブルクリックします。

プロファイル/ドメイン(Profile/Domain): プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

送信者/受信者/件名サブ文字列(Sender/Rcpt/Subject Substring): ここでは、スプールメッセージ内で検索する送信者、受信者、または件名を入力します。

受信日付(Received Date): 特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

ソート基準(Sort By): メッセージは、日付、送信者アドレス、件名、メッセージサイズを基準に並べ替えることができます。

表示数(And Show): 表示するエントリ数として、1ページあたり20エントリ、50エントリ、100エントリ、250エントリ、500エントリ、1000エントリ、またはすべてのメッセージを選択することができます。すべてのメッセージの表示には時間がかかる場合があります。

各メッセージの前にあるチェックボックスを使用するか、メッセージをクリックして、選択したメッセージにアクションを適用します。次の作業を実行できます。

- **ダウンロード(Download)**: 選択されたメッセージをダウンロードします。
- **再試行(Retry)**: 選択されたメッセージの配信を即時に再試行します。
- **削除(Delete)**: 選択されたメッセージを削除します。これを取り消すことはできません。
- **バウンス(Bounce)**: 選択されたメッセージをバウンスします。送信者には、メッセージの配信がキャンセルされたことを伝えるメッセージが送信されます。

グローバルクリーンアップアクションの選択(Select Global Cleanup Action): ここには、メッセージに対してグローバルに適用される再試行オプションとさまざまな削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

警告 - メッセージの削除を取り消すことはできません。

10.6.1.3SMTPログ

【*SMTPログ(SMTP Log)*】には、SMTP経由で処理されたすべてのメッセージのログメッセージが表示されます。

結果フィルタ(Result Filter): 表示されるメッセージのタイプを選択するには、該当するチェックボックスにチェックを入れます。

- **配信済み(Delivered)**: 配信が成功したメッセージ。
- **リジェクト(Rejected)**:ASGに拒否されたメッセージ。
- **隔離済み(Quarantined)**: 隔離されたメッセージ。
- **ブラックホール化(Blackholed)**: 通知なしで削除されたメッセージ。
- **キャンセル済み(Canceled)**:*SMTPスプール*に手動でバウンスされたメッセージ。
- **バウンス済み(Bounced)**: ルーティング設定が正しくないなどの理由により、配信できないメッセージ。
- **削除済み(Deleted)**: 手動で削除されたメッセージ。
- **不明(Unknown)**: ステータスが不明なメッセージ。

*【結果フィルタ(Result Filter)】*アイテムの選択/選択解除を切り替えるには、チェックボックスを使用します。アイテムをダブルクリックすると、そのアイテムだけが選択されます。

理由フィルタ(Reason Filter): メッセージログの表示をさらにフィルタするには、チェックボックスを使用します。

> **ヒント -** メッセージログを表示するには、メッセージログをダブルクリックします。IPアドレスを解決するには、メッセージのサーバアイコンをクリックします。アスタリスク(*)は、リバースDNSルックアップが成功したことを示します。

プロファイル/ドメイン(Profile/Domain): プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

IP/ネット/アドレス/件名 サブ文字列(IP/Net/Address/Subj. Substring): ここでは、SMTPログメッセージ内で検索するIPアドレス、ネットワークアドレス、または件名を入力します。

受信日付(Received Date): 特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダアイコンで日付を選択します。

ソート基準(Sort By): メッセージは、イベント時間、送信者アドレス、メッセージサイズを基準にソートできます。

表示数(And Show): 表示するエントリ数として、1ページあたり20エントリ、50エントリ、100エントリ、250エントリ、500エントリ、1000エントリ、またはすべてのメッセージを選択することができます。すべてのメッセージの表示には時間がかかる場合があります。

10.6.2グローバル

*【メールマネージャ(Mail Manager)】>>【グローバル(Global)】*タブの上部では、*【新しいウィンドウでメールマネージャを開く(Open Mail Manager in New Window)】*ボタンをクリックしてメールマネージャを開くことができます。

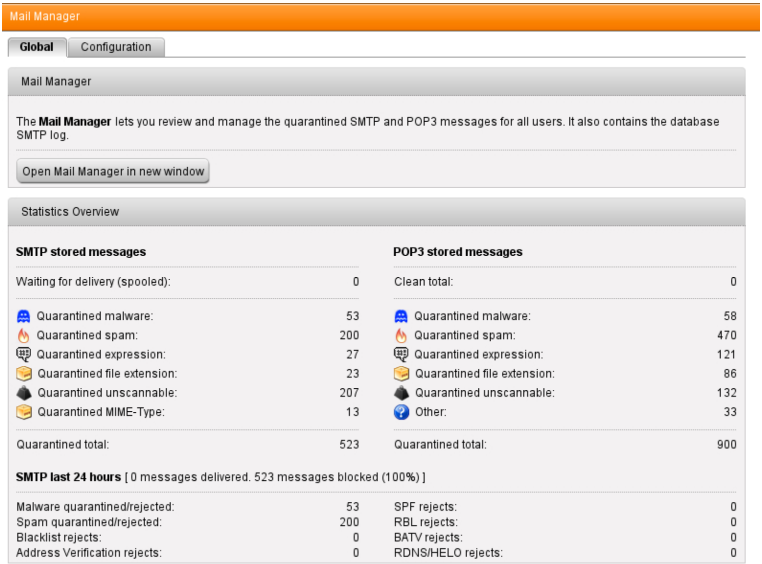


図121 メールマネージャ: 概要

下部にある【*統計概要(Statistics Overview)*】エリアには、ユニットに現在保存されているすべてのメッセージの概要が表示されます。データはSMTPプロトコル経由かPOP3プロトコル経由かによって分類されています。両方のタイプに対して、次の情報が表示されます。

- **配信待ち(スプール中)(Waiting for Delivery(Spooled))**(SMTPのみ):スキャン中なのでまだ配信できないなどの理由により、現在スプールにあるメール。
- **クリーン合計(Clean total)**(POP3のみ):ユニットがプリフェッチし、クライアント/ユーザがまだ回収していないメール。
- **隔離マルウェア(Quarantined Malware)**: ウイルスやその他の危険なコンテンツなどのマルウェアを含むメッセージの総数。
- **隔離スパム(Quarantined Spam)**: スパムと特定されたメッセージの総数。
- **隔離表現(Quarantined Expression)**: 許可されない表現が含まれるために隔離に移されたメッセージの総数。
- **隔離ファイル拡張子(Quarantined File Extension)**: 疑わしい添付ファイルが含まれるために隔離されたメッセージの総数(ファイル拡張子で識別)。
- **隔離スキャン不可(Quarantined Unscannable)**: スキャンできないため隔離されたメッセージの総数。

- **隔離MIMEタイプ(Quarantined MIME Type)**(SMTPのみ):SMTP設定に従ってフィルタすべきMIMEタイプが含まれるため隔離されたメッセージの総数。
- **総隔離数(Quarantined Total)**: 隔離されたメッセージの総数。

注 -【*配信待ち(Waiting for Delivery)*】の数は、SMTPメッセージの場合はリアルタイムのスナップショットを表します。ただしPOP3メッセージの場合は、表示される数は、前回プリフェッチが有効にされたときからの累積数です。

下に、過去24時間以内のSMTP隔離および拒否(リジェクト)の簡単な統計が表示されます。

- **マルウェア隔離/リジェクト(Malware Quarantined/Rejected)**: 有害なコンテンツが含まれるため隔離/拒否されたメッセージの数。
- **スパム隔離/リジェクト(Spam Quarantined/Rejected)**: スパム認定されたため隔離/拒否されたメッセージの数。
- **ブラックリストリジェクト(Blacklist Rejects)**: 送信者がブラックリストに含まれているため拒否されたメッセージの数。
- **アドレス検査リジェクト(Address Verification Rejects)**: 送信者アドレスを検証できなかったため拒否されたメッセージの数。
- **SPFリジェクト(SPF Rejects)**: 送信ホストが許可されないため拒否されたメッセージの数。
- **RBLリジェクト(RBL Rejects)**: 送信者がリアルタイムブラックホールリストに含まれているため拒否されたメッセージの数。
- **BATVリジェクト(BATV Rejects)**:BATVタグを検証できなかったために拒否されたメッセージの数。
- **RDNS/HELOリジェクト(RDNS/HELO Rejects)**:HELOが無効であるかRDNSエントリが不足しているために拒否されたメッセージの数。

拒否があるかどうかは【*メールセキュリティ(Mail Security)*】>>【*SMTP*】での設定に依存します。

10.6.3設定

【*メールマネージャ(Mail Manager)*】>>【*設定(Configuration)*】タブでは、データベースログをどれくらいの期間保存するのか、そして隔離メッセージを何日後に隔離場所から削除するのかを設定することができます。有効期限設定の日数を超えたログとメッセージは自動的に削除されます。

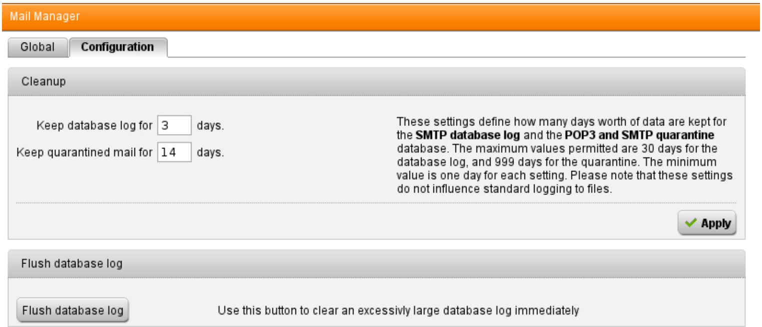


図122 メールマネージャ: 設定

デフォルト設定は次のとおりです。

- データベースログは3日経過後に削除されます。許可される最大日数は30日です。
- 隔離メッセージは14日経過後に削除されます。許可される最大日数は999日です。

データベースログと隔離の両方に対して許可される最低日数は1日です。

データベースログのフラッシュ(Flush Database Log)

このオプションは、データベースログに大量のデータが蓄積された場合にログを即時消去するときに便利です。これを使用すれば、通常のクリーンアップアクションが実行されるまで待つ必要はありません。

１１ワイヤレスセキュリティ

【*ワイヤレスセキュリティ(Wireless Security)*】メニューを使用して、Astaro Security Gatewayのワイヤレスアクセスポイント、対応するワイヤレスネットワーク、ワイヤレスアクセスを利用するクライアントを設定および管理することができます。アクセスポイントはASG上で自動的に設定されるため、個別に設定する必要はありません。アクセスポイントの設定およびステータス情報を交換するために使用される、ASGとアクセスポイントの間の通信は、AESを使用して暗号化されます。

重要 - アクセスポイントが激しく点滅している場合は、電源を切断しないでください。激しい点滅は、ファームウェアフラッシュが現在行われていることを意味します。ファームウェアフラッシュは、ワイヤレスセキュリティ更新に伴うASGシステム更新の後などに実行されます。

この章には次のトピックが含まれます。

- グローバル設定
- ワイヤレスネットワーク
- アクセスポイント
- ワイヤレスクライアント

「ワイヤレスセキュリティの概要」ページは、接続されたアクセスポイント、そのステータス、接続されたクライアント、およびワイヤレスネットワークに関する基本情報を示します。

ライブログ

【*ワイヤレスセキュリティのライブログを開く(Open Wireless Security Live Log)*】ボタンをクリックすると、アクセスポイントおよび接続を試行するクライアントに関する詳細な接続およびデバッグ情報が表示されます。

１１.１グローバル設定

【*ワイヤレスセキュリティ(Wireless Security)*】>>【*グローバル設定(Global Settings)*】ページでは、ワイヤレスセキュリティの有効化、ワイヤレスセキュリティ用のネットワークインタフェースの設定、およびWPA/WPA2エンタープライズ認証の設定が可能です。

11.1.1グローバル設定

*【ワイヤレスセキュリティ(Wireless Security)】>>【グローバル設定(Global Settings)】>>【グローバル設定(Global Settings)】*タブで、ワイヤレスセキュリティを有効または無効にできます。

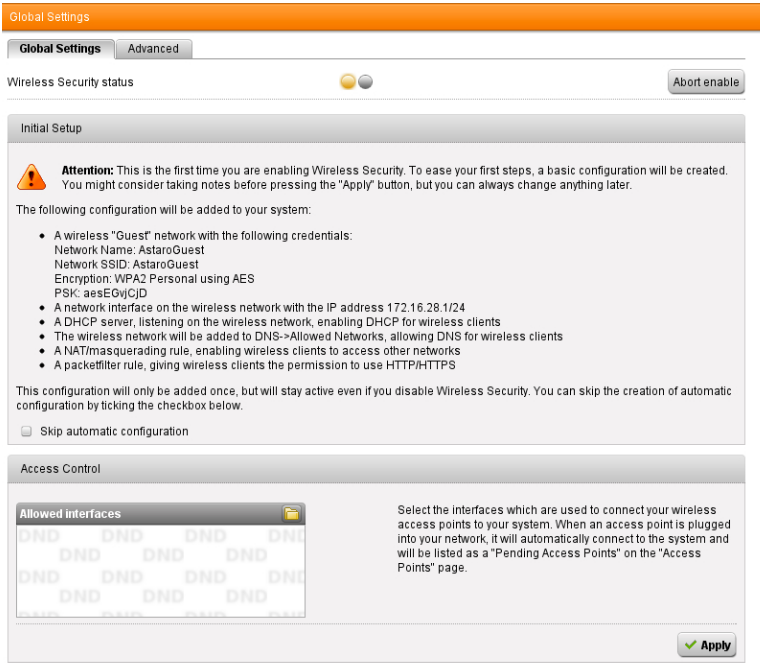


図123 ワイヤレスセキュリティ(Wireless Security):グローバル設定

ワイヤレスセキュリティを有効にするには、次の手順に従います。

1. ***【グローバル設定(Global Settings)】*タブで、ワイヤレスセキュリティを有効化します。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【アクセスコントロール(Access Control)】*エリアが編集可能になります。

   ワイヤレスセキュリティを初めて有効化する際は、*【初期セットアップ(Initial Setup)】*セクションが表示されます。ここには、作成される設定が表示されています。WPA2個人暗号

化をDHCP用ワイヤレスクライアントで使用する個別のワイヤレス「ゲスト」ネットワーク。ASGおよび*Webサーフィン*サービスでDNSを使用することが許可されます。事前共有鍵は自動生成され、このセクションのみに表示されます。初期設定はテンプレートとして機能します。いつでも*【ワイヤレスセキュリティ(Wireless Security)】>>【ワイヤレスネットワーク(Wireless Networks)】*ページで設定を編集することができます。

自動設定のスキップ(Skip Automatic Configuration): また、このオプションを選択して、初期セットアップをスキップすることもできます。この場合、ワイヤレス設定を手動で設定する必要があります。

2. **アクセスポイント用のネットワークインタフェースを選択します。**
   アクセスポイントをプラグインする設定済みインタフェースを選択するには、*【許可されるインタフェース(Allowed Interfaces)】*セクションのフォルダアイコンをクリックします。

3. ***【適用(Apply)】*をクリックします。**

   設定が保存されます。ステータスアイコンが緑色になり、ワイヤレスセキュリティが有効になります。

   設定されたネットワークインタフェースにアクセスポイントをプラグインして、続行することができます。自動設定のスキップを選択した場合は、*【ワイヤレスネットワーク(Wireless Networks)】*ページで設定を続けます。

設定をキャンセルするには、*【有効化を中止(Abort Enable)】*またはアンバー色のステータスアイコンをクリックします。

アクセスポイントをプラグインするとすぐに、アクセスポイントはシステムに自動的に接続します。新たに接続された未設定のアクセスポイントは、*【アクセスポイント(Access Points)】*ページに*【保留中のアクセスポイント(Pending Access Points)】*としてリストされます。

11.1.2詳細

*【ワイヤレスセキュリティ(Wireless Security)】>>【グローバル設定(Global Settings)】>>【詳細(Advanced)】*タブでは、WPA/WPA2エンタープライズ認証を使用するようにアクセスポイントを設定したり、VLANの使用を有効化することができます。

エンタープライズ認証

このためには、RADIUSサーバのいくつかの情報を入力する必要があります。APは認証のためにRADIUSサーバと通信せず、ASGとだけ通信します。ASGとAPの間のRADIUS通信にはポート`414`が使用されます。

WPA/WPA2エンタープライズ認証を使用にするには、次の設定を行います。

RADIUSサーバ(RADIUS Server): クライアントが自己認証を行うサーバを選択または作成します(Active Directoryサーバなど)。

RADIUSポート(RADIUS Port)(オプション):デフォルトでは、RADIUSポート1812が選択されています。必要であれば、ポートを変更できます。

RADIUSシークレット(RADIUS Secret): アクセスポイントがRADIUSサーバと通信するために必要なRADIUSパスフレーズを入力します。

シークレットの繰り返し(Repeat Secret): セキュリティ上の理由で、ここでRADIUSパスフレーズをもう一度入力します。

設定を保存するには【*適用(Apply)*】をクリックします。

VLAN設定(VLAN Settings)

このセクションでは、ワイヤレスネットワークとアクセスポイント(AP)に対してVLANの使用を有効化することができます。VLANはデフォルトでは無効になっています。

VLANセットアップは、アクセスポイントを同じネットワーク内に配置したまま、異なるスイッチやASGネットワークインタフェースに接続したい場合に便利です。

ネットワーク内のアクセスポイントに対してVLANの使用を導入するには、以下の手順に従います。

1. VLANを有効化し、VLAN IDを設定します。
2. 標準LANを使用して、APをASGに1分以上接続します。これは、APが設定を取得するために必要です。最初からVLAN経由で接続すると、APはVLAN内にあることを認識しないため、設定を取得するためにASGに接続することができません。
3. 設定を受信した後で、APを希望するVLAN(スイッチなど)に接続します。

VLANを使用したいアクセスポイントすべてについて、ステップ2と3を繰り返す必要があります。

注 VLANタギングが設定されている場合、APは設定されたVLANに対してDHCPを60秒間試行します。この時間内にIPアドレスを受信できなかった場合、APはフォールバックとして標準のLANにDHCPを試みます。

VLANタギング(VLAN Tagging): VLANを有効化するには、ドロップダウンリストから【*有効(Enabled)*】を選択します。

AP VLAN ID: アクセスポイントで使用するVLANのIDを入力します。VLANタグ0および1は使用しないでください。一般に、これらのタグはネットワークハードウェア(スイッチなど)上で特別な意味を持ちます。原則的に、4095は予約されています。

設定を保存するには*【適用(Apply)】*をクリックします。接続されたアクセスポイントは、それぞれ設定または設定の更新を受信します。その後、*【AP LANへのブリッジ(Bridge to AP LAN)】*によってワイヤレスネットワークに接続されたAPおよびワイヤレスクライアントは、通信のためにAP VLAN IDを使用します。ただし、各ワイヤレスネットワークに対して*【ワイヤレスネットワーク(Wireless Networks)】*ページの*【VLANへのブリッジ(Bridge to VLAN)】*オプションを設定することにより、単一の(あるいはすべての)ワイヤレスネットワークでこのVLAN以外のVLAN IDを使用することができます。

VLANタギングが設定されており、APがVLAN経由でASGにコンタクトできない場合、APは自動的にリブートし、設定の受信後に再試行します。

注 -VLANを無効化した場合、*【VLANへのブリッジ(Bridge to VLAN)】*オプションを使用するすべてのワイヤレスネットワークは*【AP LANへのブリッジ(Bridge to AP LAN」】*にリセットされます。

11.2ワイヤレスネットワーク

*【ワイヤレスセキュリティ(Wireless Security)】>>【ワイヤレスネットワーク(Wireless Networks)】*ページでは、ワイヤレスネットワークを定義できます(SSIDおよび暗号化方式など)。さらに、ワイヤレスネットワークに個別のIPアドレス範囲が必要か、アクセスポイントのLANに対するブリッジングが必要かを定義することができます。

図124 ワイヤレスセキュリティ(Wireless Security):ワイヤレスネットワーク

新しいワイヤレスネットワークを作成するには、次の手順に従います。

1. ***【ワイヤレスネットワーク(Wireless Networks)】ページで【ワイヤレスネットワークの追加(Add Wireless Network)】をクリックします。***
   *【ワイヤレスネットワークの追加(Add Wireless Network)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
ネットワーク名前(Network Name): ネットワークを説明する名前を入力します。

ネットワークSSID(Network SSID): ワイヤレスネットワークの識別のためにクライアントに表示される、ネットワークのサービスセット識別子(SSID)を入力します。SSIDは、1～32文字のASCII印字可能文字[1]で構成します。コンマは使用できず、先頭または末尾をスペースにすることはできません。

暗号化モード(Encryption Mode): ドロップダウンリストから暗号化モードを選択します。デフォルトは*WPA2 Personal*です。セキュリティ上の理由から、ワイヤレスネットワークを使用しているクライアントの中に、WEP以外の方法をサポートしないクライアントがいなければ、WEPを使用しないことを推奨します。エンタープライズ認証方式を使用する場合、【*グローバル設定(Global Settings)*】>>【*詳細(Advanced)*】タブでRADIUSサーバも設定する必要があります。

パスフレーズ/PSK(Passphrase/PSK): *WPA/WPA2 Personal*暗号化モードのみで使用できます。許可されないアクセスからワイヤレスネットワークを保護するパスフレーズを入力し、次のフィールドに再入力してください。パスフレーズには、8～63文字のASCII印字可能文字を使用します。

アルゴリズム(Algorithm): WPA/WPA2のみで使用できます。暗号化アルゴリズムを*AES*または*TKIP & AES*から選択します。

128ビットのWEPキー(128-bit WEP Key): *WEP*暗号化モードのみで使用できます。ここで、26文字ちょうどの16進文字から成るWEPキーを入力します。

クライアントトラフィック(Client Traffic): ワイヤレスネットワークをローカルネットワークに統合する方法を選択します。

- **分離ゾーン(Separate Zone)**(デフォルト): ワイヤレスネットワークは、独自のIPアドレス範囲を持つ独立したネットワークとして処理されます。

> **注 -** 既存の*分離ゾーン*ネットワークを【*APLANへのブリッジ(Bridge to AP LAN)*】または【*VLANへのブリッジ(Bridge to VLAN)*】に切り替えると、ASG上の設定済みWLANインタフェースは*未割り当て*になります。ただし、編集して再有効

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

化することにより、新しいハードウェアインタフェースをインタフェースオブジェクトに割り当てることができます。

- **AP LANへのブリッジ(Bridge to AP LAN)**: ワイヤレスネットワークをアクセスポイントのネットワークにブリッジングすることができます。つまり、ワイヤレスクライアントは同じIPアドレス範囲を共有します。

  注 - VLANが有効な場合、ワイヤレスクライアントはアクセスポイントのVLANネットワークにブリッジングされます。

- **VLANへのブリッジ(Bridge to VLAN)**: VLANが有効な場合、このワイヤレスネットワークのトラフィックを任意のVLANにブリッジングさせることができます。これは、ワイヤレスクライアントから独立した共通ネットワーク内にアクセスポイントを含めたい場合に便利です。
  VLAN IDへのブリッジ(Bridge to VLAN ID): ワイヤレスクライアントが含まれるネットワークのVLAN IDを入力します。

  クライアントVLAN ID(Client VLAN ID): VLAN IDの定義方法を選択します。

  - **スタティック(Static)**:【*グローバル設定(Global Settings)*】>>【*詳細(Advanced)*】ページに定義されたVLAN IDを使用します。
  - **RADIUSおよびスタティック(RADIUS & Static)**:RADIUSサーバが提供するVLAN IDを使用します。ユーザがいずれかのワイヤレスネットワークに接続し、RADIUSサーバで認証を行うと、RADIUSサーバはこのユーザに対して使用すべきVLAN IDをアクセスポイントに知らせます。したがって、複数のワイヤレスネットワークを使用する際に、どのユーザがどの内部ネットワークにアクセスできるのかをユーザごとに定義することができます。ユーザにVLAN ID属性が割り当てられていない場合、【*グローバル設定(Global Settings)*】>>【*詳細(Advanced)*】ページで定義されたVLAN IDが使用されます。

クライアント隔離(Client Isolation): ネットワーク内のクライアントは通常、互いに通信できます。ゲストネットワーク内などでこれを禁止したい場合、ドロップダウンリストで【*有効(Enabled)*】を選択します。

SSID非表示(Hide SSID): SSIDを非表示にしたい場合があります。これには、ドロップダウンリストから【*はい(Yes)*】を選択します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   設定が保存され、ワイヤレスネットワークが*【ワイヤレスネットワーク(Wireless Networks)】*リストに表示されるようになります。

各ワイヤレスネットワークに対して分離ゾーンを使用すると、対応するハードウェアオブジェクト(*wlan0*など)はバックグラウンドで作成されます。これにより、ネットワークインタフェースを作成し、ワイヤレスネットワークのIPアドレス範囲を定義することができます。次に、このネットワークインタフェースをASGの各種設定で使用することができます。具体的には、ワイヤレスネットワークに対し、DHCPサーバ、ファイアウォールルール、マスカレードルールなどを作成することができます。

11.3アクセスポイント

【ワイヤレスセキュリティ(Wireless Security)】>>*【アクセスポイント(Access Points)】*ページは、システムで認識されているアクセスポイント(AP)の概要を示します。Astaro Security Gatewayは、アクティブ、無効、保留中のAPを識別します。本物のAPのみがネットワークに接続するようにするために、まず、APを承認する必要があります。

ヒント - このページの3つのセクションは、セクションヘッダの右にあるシンボルをクリックして折り畳んだり、再び展開することができます。

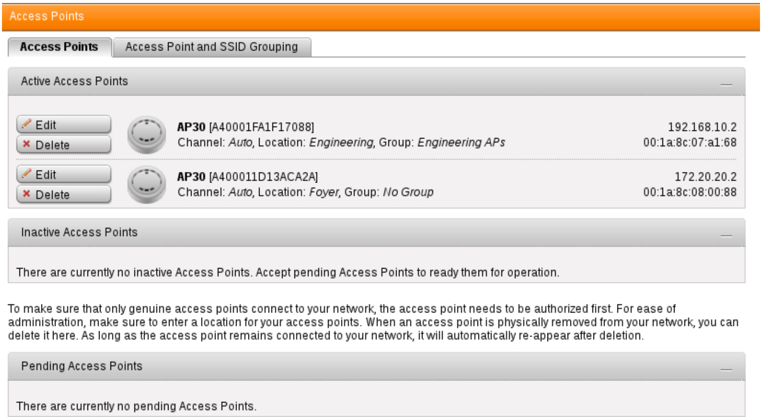


図125 ワイヤレスセキュリティ:アクセスポイント

簡単に管理できるように、各APの場所を入力することができます。また、ここでは、チャネルを変更することもできます。チャネルを【*自動(Auto)*】のままにすると、APは一番使用されていないチャネルで自動的に送信されます。APに変更を加えるには、【*編集(Edit)*】ボタンをクリックします。

APをネットワークから物理的に削除する場合、ここで【*削除(Delete)*】ボタンをクリックして削除します。APがネットワークに接続されている限り、削除後も【*保留中(Pending)*】状態で自動的に再表示されます。

注 - 設定の変更後、すべてのインタフェースが再設定されるまで約15秒必要です。

アクティブなアクセスポイント(Active Access Points)

ここには、接続されており設定済みで実行中のAPがリストされます。

無効なアクセスポイント(Inactive Access Points)

ここには、過去に設定されていたが現在はASGに接続されていないAPがリストされます。APがこの状態で5分間経過した場合、APのネットワーク接続とシステムの設定を確認してください。ワイヤレスセキュリティサービスを再起動すると、「*最後の表示(Last seen)*」タイムスタンプが消去されます。

保留中のアクセスポイント(Pending Access Points)

ここには、システムに接続されているが未承認のAPがリストされます。アクセスポイントを承認するには、各アクセスポイントで【*同意(Accept)*】ボタンをクリックしてください。承認済みのアクセスポイントは、現在アクティブであるか否かに応じて、上のいずれかのセクションに即時に表示されます。

注 - 保留中のAPに対して【*同意(Accept)*】をクリックすると、ネットワーク内のすべてのSPがリブートされます。

11.3.1 アクセスポイントおよびSSIDグルーピング

*【ワイヤレスセキュリティ(Wireless Security)】>>【アクセスポイント(Access Points)】>>【アクセスポイントおよびSSIDグルーピング(Access Point and SSID Grouping)】*ページでは、複数の方法でアクセスポイント(AP)を管理することができます。1番目の方法では、ワイヤレスネットワークをアクセスポイントに割り当てて、各アクセスポイントで専用ワイヤレスネットワークのみをブロードキャストします。これは、オフィスにのみブロードキャストすべき会社のワイヤレスネットワークや、建物内の公共部分のみでブロードキャストすべきゲストワイヤレスネットワークなどで便利です。

2番目の方法では、アクセスポイントをグループ化します。これらのグループにはワイヤレスネットワークのみを割り当てることができます。

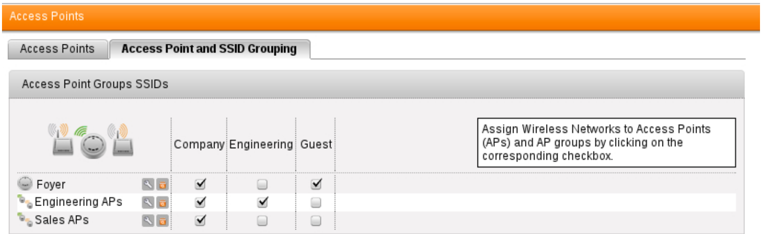


図126 ワイヤレスセキュリティ: アクセスポイントおよびSSIDグルーピング

このページには、ワイヤレスネットワーク、アクセスポイント、およびアクセスポイントグループ(存在する場合)とその相互関係の組み合わせが表示されます。

各APまたはAPグループの横には、編集およびゴミ箱のアイコンがあります。編集アイコンを使用すると、APまたはグループの属性を変更できます。ゴミ箱アイコンをクリックすると、グループまたはアクセスポイントが削除されます。

ワイヤレスネットワークの設定を編集するには、ワイヤレスネットワーク名をクリックしますs.

APへのネットワーク割り当て

APまたはAPグループにワイヤレスネットワークを割り当てるには、それぞれのチェックボックスをオンにします。AP(またはグループ内のすべてのAP)は、割り当てられたすべてのワイヤレスネットワークをブロードキャストします。

また、【編集(Edit)】ダイアログウィンドウでは、APの場所やチャネルを変更することもできます。

グループの作成と使用

APグループを作成するには、APの編集アイコンをクリックします。*【グループ(Group)】*ドロップダウンリストで*【新規グループ(New Group)】*を選択し、*【名前(Name)】*フィールドに名前を入力します。*【保存(Save)】*をクリックします。APのリストに新しいグループが表示され、APはグループの一部となったためリストに表示されなくなります。

> **ヒント - **APまたはグループの名前をクリックしても、【編集(Edit)】ダイアログウィンドウにアクセスすることができます。

APの編集アイコンをクリックし、*【グループ(Goup)】*ドロップダウンリストでグループを選択することで、グループにAPを追加することができます。

グループからAPを削除するには、当該グループの編集アイコンをクリックし、グループから削除したいAPの前にあるゴミ箱アイコンをクリックします。

また、【編集(Edit)】ダイアログウィンドウでグループの名前を変更することもできます。

11.4ワイヤレスクライアント

*【ワイヤレスセキュリティ(Wireless Security)】>>【ワイヤレスクライアント(Wireless Clients)】*ページは、現在アクセスポイントに接続されている(または過去に接続されていた)クライアントの概要を示します。

図127 ワイヤレスセキュリティ(Wireless Security):クライアント

すべてのクライアントが名前を送信する訳ではないため、ここで名前を割り当てて、概要で既知のクライアントを識別しやすくできます。クライアントがDHCP要求中にNetBIOS名を送信する場合、この名前がテーブルに表示されます。送信しない場合、クライアントはリストに*[unknown]*(不明)と表示されます。これらの不明クライアントの名前は、名前の前にある鍵アイコンをクリックして変更することができます。次に、名前を入力して*【保存(Save)】*をクリックします。変更が有効になるまで数秒かかります。WebAdminの右上隅にある【リロード(Reload)】ボタンから、クライアントの名前を参照できます。

また、テーブルで最初の列にあるゴミ箱アイコンをクリックして、クライアントをテーブルから削除することもできます。

ワイヤレスセキュリティサービスを再起動すると、「*最後の表示(Last seen)*」タイムスタンプが消去されます。

> **注 -** クライアントに割り当てられたIPアドレスは、ASGが該当ワイヤレスネットワークのDHCPサーバとして機能する場合にのみ表示可能です。さらに、スタティックDHCPマッピングのために、現時点ではIPアドレス`0.0.0.0`が表示されます。

１２Webアプリケーションセキュリティ

この章では、Webサーバを攻撃や悪意ある行為から保護するAstaro Security GatewayのWebアプリケーションファイアウォールを設定する方法を説明します。

この章には次のトピックが含まれます。

- Webアプリケーションファイアウォール
- 証明書管理

１２.１Webアプリケーションファイアウォール

Astaro Security GatewayでWebアプリケーションファイアウォール(WAF、あるいはリバースプロキシ)を使用すると、Webサーバをクロスサイトスクリプティング(XSS)、SQLインジェクション、ディレクトリトラバーサルなどの攻撃や悪意ある行為、あるいはその他の潜在的な攻撃から防御することができます。DNATルールを使用して実際のマシンに変換される外部アドレス(仮想サーバ)を定義することができます。ここで、様々なパターンと検出方法を使用して、サーバを保護することができます。簡単に言うと、ASGのこのエリアでは、Webサーバから送受信される要求に、利用条件を適用することができます。また、複数のターゲットに対する負荷分散が可能です。

１２.１.１グローバル

*【Webアプリケーションファイアウォール(Web Application Firewall)】>>【グローバル(Global)】*タブでは、Webアプリケーションファイアウォール(WAF)を有効または無効にできます。

> **注 -** WAFを有効にする前に、*【仮想Webサーバ(Virtual Web Servers)】*タブで仮想Webサーバを1つ以上作成する必要があります。

WAFを有効にするには、次の手順に従います。

1. **リアルWebサーバまたは仮想Webサーバを1つ以上作成します。**
   詳しくは、「*リアルWebサーバ*」と「*仮想Webサーバ*」のセクションを参照してください。

2. **Webアプリケーションファイアウォールを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンが緑色になり、Webアプリケーションファイアウォールが有効になります。

ライブログ

WAFライブログは、WAFイベントに関するデバッグ情報を提供します。【*ライブログを開く(Open Live Log)*】ボタンをクリックすると、新しいウィンドウでライブログが開きます。

12.1.2仮想Webサーバ

【*Webアプリケーションファイアウォール(Web Application Firewall)*】>>【*仮想Webサーバ(Virtual Web Servers)*】タブでは、仮想Webサーバを作成できます。これらのWebサーバは、ASGの一部として、インターネットとWebサーバの間のファイアウォールを構築します。そのため、このような介入をリバースプロキシとも呼びます。ASGは、Webサーバへの要求をピックアップし、リアルWebサーバを様々な攻撃から保護します。それぞれの仮想サーバはリアルWebサーバにマッピングされており、どのような保護レベルを適用するかを決定します。また、複数のリアルWebサーバを1つの仮想Webサーバ定義で使用することもできます。これにより、リアルWebサーバの負荷分散を実行できます。

仮想サーバを追加するには、次の手順に従います。

1. **【*仮想Webサーバ(Virtual Web Servers)*】ボタンをクリックします。**
   【*新規仮想Webサーバを作成(Create Virtual Web Server)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): 仮想Webサーバを説明する名前を入力します。

   タイプ(Type): クライアントと仮想Webサーバの間の通信を暗号化するか(HTTPS)しないか(HTTP)を決定します。

   ドメイン(Domains)(*HTTPのみ*):Webサーバが責任を持つドメインをFQDNとして入力します(例:`shop.example.com`)。

   証明書(Certificate)(*HTTPSのみ*):ドロップダウンリストからWebサーバの証明書を選択します。証明書は事前に作成しておく必要があります。

      ドメイン(Domain):このフィールドには、証明書の作成されるホスト名が表示されます。

ドメイン(Domains)(SAN証明書のみ):WAFは、SAN(Subject Alternative Name)証明書をサポートします。証明書でカバーされるすべてのホスト名がこのボックスにリストされます。続いて、ホスト名の前にあるチェックボックスにチェックを入れて、複数のホスト名を選択することができます。

インタフェース(Interface): ドロップダウンリストから、Webサーバへの到達が可能なインタフェースを選択します。

ポート(Port): 仮想Webサーバに外部から到達可能なポート番号を入力します。デフォルトはポート80(*HTTP*)とポート443(*HTTPS*)です。

リアルWebサーバ(Real Web Servers): ファイアウォールプロファイルを適用するWebサーバの前にあるチェックボックスにチェックを入れます。ミラーリングWebサーバがある場合、複数のWebサーバを選択することもできます。続いて、トラフィックは選択したWebサーバに負荷分散されます。

ファイアウォールプロファイル(Firewall Profile): ドロップダウンリストからファイアウォールプロファイルを選択します。このプロファイルは、選択したWebサーバを保護するために適用されます。また、ファイアウォールプロファイルを一切使用しない場合は【*なし(None)*】を選択できます。

HTML書き換えを有効化(Enable HTML Rewriting)(オプション)このオプションを選択すると、返されたWebページのリンクをASGが書き換えるため、リンクが有効に保たれます。例:リアルWebサーバのインスタンスの1つが、`yourcompany.local`というホスト名であるが、ASGでの仮想サーバのホスト名が`yourcompany.com`である。したがって、`<a href="http://yourcompany.local/">`のような絶対リンクは、クライアントへの配信前にリンクを`<a href="http://yourcompany.com/">`に書き換えなければ破損してしまいます。ただし、Webサーバで`yourcompany.com`が設定されているか、Webページの内部リンクが常に相対リンクとして表現されている場合には、このオプションを有効にする必要はありません。MicrosoftのOutlook Web AccessやSharepoint Portal Serverでは、このオプションを使用することを推奨します。

> **注 -** 一部のリンクが正しく書き換えられず、無効となる場合もあります。リンクを一貫してフォーマットするよう、Webサイトの作者に依頼してください。

URL書き換えとは別に、HTML書き換え機能でも、正しくフォーマットされていないHTMLを次のように修正することができます。

- DOMツリーで、<title>タグを、ノード`html > title`から正しい`html > head > title`に移動する

- HTML属性値を囲む引用符を修正する(例:`name="value""`が`name="value"`になる)

クロスリファレンス - 詳しくは、libxmlドキュメントを参照してください(http://xmlsoft.org/html/libxml-HTMLparser.html)。

パスホストヘッダ(Pass Host Header)(オプション):このオプションを選択すると、クライアントに要求されたホストヘッダが保持され、Web要求とともにWebサーバへ転送されます。環境内で、ホストヘッダの受け渡しが必要かどうかは、Webサーバの設定に応じて決まります。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   サーバが*【仮想Webサーバ(Virtual Web Servers)】*リストに追加されます。

仮想サーバに複数のWebサーバが設定されている場合、*【仮想Webサーバ(Virtual Web Servers)】*リストには、各Webサーバのステータスアイコンが表示されます。Webサーバのステータスアイコンは、サーバが有効でない場合は赤くなります。Webサーバがダウンしているか利用できない場合は黄色、すべて正常に機能している場合は緑色です。

12.1.3リアルWebサーバ

*【Webアプリケーションファイアウォール(Web Application Firewall)】>>【リアルWebサーバ(Real Web Servers)】*タブで、WAFによって保護するWebサーバを追加できます。Webサーバは、自動的にまたは手動で追加します。

Webサーバを自動的に追加するには、次の手順に従います。

1. ***【Webサーバの検出(Discover Web Servers)】*ボタンをクリックします。**
   情報ダイアログウィンドウが開きます。

2. ***【OK】*をクリックします。**
   情報ダイアログウィンドウが閉じて、検出プロセスがバックグラウンドで起動します。

3. **WebAdmin上部の【リロード(Reload)】ボタンを押して、結果を参照します。**
   検出プロセスには数分ほどかかる場合があります。Webサーバは、ASGと同じネットワーク内にある場合のみ、検出可能です。

   Webサーバが検出されたら、*【仮想Webサーバ(Virtual Web Servers)】*タブでこれらのサーバにファイアウォールプロファイルを割り当てることができます。一部のWebサーバだけ

検出された場合や、Webサーバが全く検出されなかった場合には、以下の手動による方法に従ってください。

Webサーバを手動で追加するには、次の手順に従います。

1. ***【新規のリアルWebサーバ(New Real Web Servers)】*ボタンをクリックします。**
   *【新規リアルWebサーバを作成(Create Real Web Server)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): Webサーバを説明する名前を入力します。

   ホスト(Host): ホストを追加または選択します。ホストは、タイプが「*ホスト(Host)*」または「*DNSホスト(DNS Host)*」です。ここでは、DNSホスト名の使用を強く推奨します。これは、IPアドレスでリストされたホストは空のホストヘッダを送信するため、一部のブラウザで問題が発生するためです。

   タイプ(Type):ASGとWebサーバの間の通信を暗号化するか(HTTPS)しないか(HTTP)を決定します。

   ポート(Port):ASGとWebサーバの間の通信に使用するポート番号を入力します。デフォルトはポート80(*HTTP*)とポート443(*HTTPS*)です。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
   サーバが*【リアルWebサーバ(Real Web Servers)】*リストに追加されます。

これで*【仮想Webサーバ(Virtual Web Servers)】*タブで存在するWebサーバをファイアウォールプロファイルに割り当てることが可能になりました。

12.1.4ファイアウォールプロファイル

*【Webアプリケーションファイアウォール(Web Application Firewall)】>>【ファイアウォールプロファイル(Firewall Profiles)】*タブでは、Webサーバの保護モードとレベルを定義するWAFプロファイルを作成できます。

WAFプロファイルを作成するには、以下の手順に従います。

1. ***【新規ファイアウォールプロファイル(New Firewall Profile)】*ボタンをクリックします。**
   *【ファイアウォールプロファイルの作成(Create Firewall Profile)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): プロファイルの名前を入力します。

   モード(Mode): ドロップダウンリストからモードを選択します。

   - **モニタ(Monitor)**: HTTP要求をモニタリングし、ログに記録します。
   - **リジェクト(Reject)**: HTTP要求は拒否されます。
   - **破棄(Drop)**: HTTP要求は破棄されます。

   選択したモードは、HTTP要求が下で選択したいずれかの条件と合致している場合に適用されます。

   SQLインジェクションフィルタ(SQL Injection Filter): WebサーバをSQLインジェクションから保護します。このために、HTMLフォームやその他の入力フィールドが、パーサによって、SQLコマンドを使用してチェックされます。

   クロスサイトスクリプティング(XSS)フィルタ(Cross Site Scripting (XSS) Filter): Webサーバをクロスサイトスクリプティングから保護します。このために、HTMLフォームやその他の入力フィールドが、パーサによって、HTMLおよびCSSコマンドを使用してチェックされます。

   Cookie署名を有効化(Enable Cookie Signing): WebサーバをCookieの悪用から保護します。WebサーバがCookieをセットすると、最初のCookieに対して2つ目のCookieが追加されます。このCookieには、最初のCookieの名前、値、シークレットから構成されたハッシュが含まれており、シークレットはWAFによってのみ認識されます。したがって、要求によって正しいCookieペアが提供されない場合は、ある種の悪用が行われた可能性があり、Cookieは破棄されます。

   URL強化を有効化(Enable URL Hardening): URL書き換えから保護します。このために、クライアントがWebサイトを要求すると、このWebサイトのすべてのURLに対して署名が行われます。この署名手順は、Cookie署名と似ています。さらに、次にどのリンクを有効に要求できるのかについて、Webサーバからの応答が解析されます。強化されたURLをブックマークし、後でアクセスすることができます。エントリURLを定義する方法を、以下のいずれかから選択します。

   - **エントリURLを手動で指定(Entry URLs specified manually)**: WebサイトのエントリURLとして機能するURLを入力します。これにより、署名が不要になります。これらのURLは、次の例の構文に準拠している必要があります:
     `http://shop.example.com/products/`
     、`https://shop.example.com/products/`、または`/products/`

- **アップロードしたGoogleサイトマップファイルからのエントリURL(Entry URLs from uploaded Google sitemap file)**: ここで、Webサイトの構造に関する情報が含まれるサイトマップファイルをアップロードします。 サイトマップファイルは、XML形式でもプレーンテキスト形式でもアップロードできます。後者のファイルはURLのリストのみが含まれます。プロファイルを保存すると、サイトマップファイルはWAFによって構文解析されます。
- **GoogleサイトマップURLからのエントリURL(Entry URLs from Google sitemap URL)**:ASGに、Webサイトの構造に関する情報が含まれるサイトマップファイルを、定義されたURLからダウンロードさせることができます。このファイルにアップデートがないか定期的にチェックすることができます。プロファイルを保存すると、サイトマップファイルはダウンロードされ、WAFによって構文解析されます。
  URL: サイトマップへのパスを絶対URLとして入力します。

  更新(Update): ドロップダウンリストから更新感覚を選択します。【*手動(Manual)*】を選択すると、サイトマップはこのプロファイルの更新を保存した場合にのみ更新されます。

フォーム強化を有効化(Enable Form Hardening): URL書き換えから保護します。フォーム強化は、Webフォームのオリジナル構造を保持し、署名します。そのため、フォームの送信時にフォームの構造が変更されると、サーバは要求を拒否します。

アンチウイルススキャンを使用(Use AntiVirus Scanning): このオプションを選択して、Webサーバをウイルスから防御します。

AVエンジン(AV Engines):Astaro Security Gateway は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン(Single Scan)**: デフォルトの設定で、最高のパフォーマンスを提供します。
- **デュアルスキャン(Dual Scan)**: 異なるウイルススキャナを使用してすべてのEメールを2回スキャンすることで最大の認識率を提供します。

スキャン(Scan): ドロップダウンリストから、アップロードまたはダウンロードのいずれかをスキャンするか、その両方をスキャンするかを選択します。

評判の悪いクライアントをブロック(Block Clients with Bad Reputation):GeoIPおよびRBL情報に基づいて、評判の悪いクライアントを分類に従ってブロックすることができます。Astaroでは次の分類プロバイダを利用します。

RBLソース:

- Commtouch IP Reputation(ctipd.org)
- dnsbl.proxybl.org
- http.dnsbl.sorbs.net

GeoIPソースはMaxmindです。WAFは、次のいずれかのMaxmindカテゴリに属するクライアントをブロックします。

- A1:クライアントによって、IPアドレスや本来の所在地を隠すために使用される匿名プロキシまたはVPNサービス。
- A2:衛星プロバイダとは、衛星を利用して世界中の(多くの場合、高リスクな国の)ユーザにインターネットアクセスを提供しているISPです。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
   WAFルールをスキップ(Skip WAF Rules): このボックスに、誤検出などが理由で現在のプロファイルでスキップしたいWAFルール番号を追加します。これらのWAFルール番号は、*【ログおよびレポーティング(Logging & Reporting)】>>【Webアプリケーションファイアウォール(Web Application Firewall)】>>【詳細(Detail)】*ページで、*【上位ルール(Top Rules)】*フィルタを使用して取得できます。

   評判の悪いクライアントのリモートルックアップをスキップ(Skip Remote Lookups for Clients with Bad Reputation): 評判ルックアップにはリモート分類プロバイダへの要求の送信が含まれるため、評判に基づくブロック機能を使用すると、システムのパフォーマンスが低下する可能性があります。このチェックボックスは、GeoIPに基づく分類を使用する場合にのみ、チェックを入れてください。この場合、キャッシュされた情報を使用するため、パフォーマンスは大幅に向上します。

4. ***【保存(Save)】*をクリックします。**
   新しいWAFプロファイルが*【ファイアウォールプロファイル(Firewall Profiles)】*リストに追加されます。

URL強化とフォーム強化に関する追加情報

URL強化とフォーム強化の両方を有効化することを推奨します。これら2つの機能は相補的なので、いずれか一方だけ有効化した場合に起こり得る問題を解決することができます。

- フォーム強化だけ有効化した場合:Webページに、`http://example.com/?view=article&id=1`のように、クエリが追加されたハイパーリンクが含まれる場合(特定のCMSなど)、このようなページ要求はフォーム強化によってブロックされます。これは、必要な署名が存在しないためです。

- URL強化だけ有効化した場合：WebブラウザがフォームデータをWebフォームのformタグのアクションURLに追加する場合（GET要求など）、フォームデータはWebサーバに送信される要求URLの一部となり、URL署名が無効になります。

両方の機能を有効化することで問題が解決するのは、フォーム強化とURL強化のいずれかが要求を有効だとみなすと、サーバが要求を受け付けるためです。

Outlook Web Access

Outlook Web Access（OWA）用のWAFの構成はややリスクを伴います。これは、OWAがパブリックIPからの要求を、内部LAN IPからのOWA Webサイトへの要求とは別の方法で処理するためです。OWAのURLにはリダイレクトが追加されます。外部アクセスのためには外部FQDNが使用されますが、内部要求には内部サーバのIPアドレスが使用されます。

解決策は、OWAサーバのWAFプロファイルで、OWAディレクトリを*エントリURL*として設定することです（例：`http://webserver/exchange/`）。さらに、パス`/exchange/*`のURL強化をスキップする例外を作成し、Cookie署名を仮想サーバに対して完全に無効化する必要があります。

12.1.5除外

*【Webアプリケーションファイアウォール（Web Application Firewall）】>>【除外（Exceptions）】*タブでは、特定のチェックから除外されるWeb要求やソースネットワークを定義できます。

1. ***【除外（Exception）】*タブで、*【新規除外リスト（New Exception List）】*をクリックします。**
   *【除外リストを作成（Create Exception List）】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   コメント（Comment）（オプション）：説明などの情報を追加します。

   名前（Name）：除外を説明する名前を入力します。

   スキップするチェック（Skip These Checks）：スキップするセキュリティチェックを選択します。

   この仮想サーバ上（On This Virtual Server）：ドロップダウンリストから、選択されたチェックから除外する仮想Webサーバを選択します。

   全リクエストに適用（For All Requests）：ドロップダウンリストから要求定義を選択します。ANDまたはORを使用して、2つの要求の定義を論理的に組み合わせることができます。

ネットワーク(Networks): クライアント要求の発信元であり、選択されたチェックから除外するソースネットワークを追加または選択します。

パス(Paths): 選択されたチェックから除外するパスを、`/products/images/*` のような形式で追加します。

3. ***【保存(Save)】をクリックします。***
新しい除外が*【除外(Exceptions)】*リストに追加されます。

12.1.6詳細

*【Webアプリケーションファイアウォール(Web Application Firewall)】>>【詳細(Advanced)】*タブでは、cookieの署名とURL強化に使用する鍵を定義できます。

Cookie署名鍵(Cookie Signing Key)

ここでは、Cookie署名用の署名鍵として使用できるカスタムのシークレットを入力できます。

URL強化署名鍵(URL Hardening Signing Key)

ここでは、URL強化用の署名鍵として使用されるカスタムのシークレットを入力できます。

フォーム強化設定(Form Hardening Settings)

ここでは、フォーム強化トークンの暗号鍵として使用されるカスタムのシークレットを入力できます。シークレットは8文字以上にする必要があります。

12.2認証管理

*【サイト間VPN(Site-to-site VPN)】>>【証明書管理(Certificate Management)】*メニューと*【Webアプリケーションセキュリティ(Web Application Security)】>>【証明書管理(Certificate Management)】*メニューには、同じ設定オプションが含まれています。これらの設定オプションを使用すると、Astaro Security Gatewayのすべての認証関連オプションを管理することができます。たとえば、X.509証明書の作成またはインポートや、CRL*(証明書失効リスト)*のアップロードなどを行うことができます。

12.2.1証明書

*「サイト間VPN」>>「証明書管理」>>「証明書」*を参照してください。

12.2.2認証局

*「サイト間VPN」>>「証明書管理」>>「認証局」*を参照してください。

12.2.3失効リスト

*「サイト間VPN」>>「証明書管理」>>「失効リスト」*を参照してください。

12.2.4詳細

*「サイト間VPN」>>「証明書管理」>>「詳細」*を参照してください。

13REDマネジメント

この章では、Astaro REDの設定方法について説明します。REDは*リモートイーサネットデバイス(Remote Ethernet Device)*の略で、リモートオフィス(遠隔地の支店)などを、あたかもローカルネットワークの一部であるかのようにメインオフィス(本社)に接続する手段です。

セットアップは、メインオフィスのAstaro Security Gatewayとリモートオフィスのリモートイーサネットデバイス(RED)で構成されます。REDアプライアンス自体は設定する必要がないため、2拠点間の接続は非常に簡単に確立できます。REDアプライアンスは、ASGに接続するとただちに、ASG上の他のイーサネットデバイスと同じように動作します。支店のすべてのトラフィックはASGを介して安全にルーティングされるため、支店はローカルネットワークと同じように安全になります。

この章には次のトピックが含まれます。

- 概要
- グローバル設定
- デバイス設定
- 導入ヘルパ

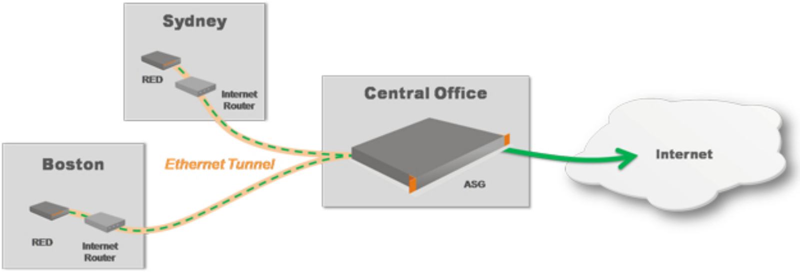


図128 RED: セットアップの略図

RED環境のセットアップは、以下の手順で行います。

1. REDサポートをアクティブにします。
2. ASG上でREDアプライアンスを設定します。
3. REDアプライアンスをリモートサイト上のインターネットに接続します。

注 – REDアプライアンスが設定されていないと、REDの概要ページには、REDアーキテクチャの一般的な情報が表示されます。REDアプライアンスを設定すると、そのページにはREDのステータスに関する情報が表示されます。

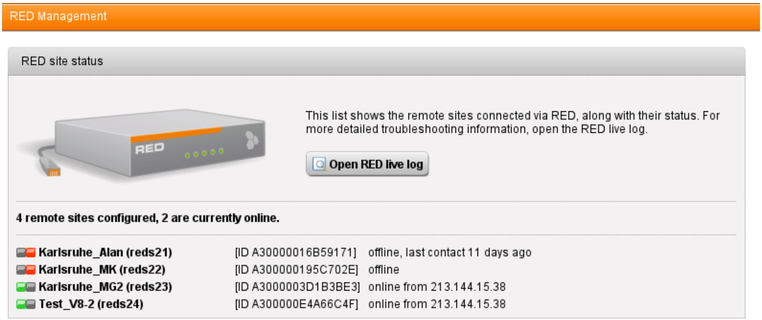


図129 RED:概要ページのサイトのステータス

REDライブログを開く(Open RED Live Log)

ライブログを使用してAstaro Security GatewayとREDアプライアンス間の接続を監視できます。【*REDライブログを開く(Open RED Live Log)*】ボタンをクリックして、新しいウィンドウでライブログを開きます。

13.1概要

【*概要(Overview)*】ページは、REDの概要、その機能、および一般的なREDのセットアップについて基本情報を示します。

13.2グローバル設定

【*グローバル設定(Global Settings)*】タブでは、REDのサポートを有効または無効にすることができます。REDのサポートを有効にすると、ASGがREDハブとして機能します。 REDサポートは、REDアプライアンスをASGに接続する前に有効にしておく必要があります。

REDサポートを有効にするには、次の手順に従います。

1. **【*グローバル設定(Global Settings)*】タブで、REDサポートを有効化します。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色になり、【*REDハブ設定(RED Hub Configuration)*】エリアが編集可能になります。

2. **組織の詳細を入力します。**
   デフォルトで、【*マネジメント(Management)*】>>【*システム設定(System Settings)*】>>【*組織(Organizational)*】タブの設定が使用されます。

3. **【*REDを有効にする(Activate RED)*】をクリックします。**
   ステータスアイコンが緑色になり、REDサポートが有効になります。これでASGがAstaroのRPS(RED Provisioning Service)に登録され、REDハブとして機能するようになります。

   【*RED*】>>【*デバイス設定(Device Configuration)*】ページで1つ以上のREDアプライアンスを追加して、続行することができます。

設定をキャンセルするには、【*有効化を中止(Abort Enable)*】またはアンバー色のステータスアイコンをクリックします。

13.3デバイス設定

【*デバイス設定(Device Configuration)*】ページでは、RED(Remote Ethernet Device)アプライアンスを手動で設定できます(エキスパートモード)。より便利な方法をお求めの場合は、次のWebAdminページにある導入ヘルパを使用してください。

ここで設定した各アプライアンスは、ASGとの接続を確立できるようになります。

注 - REDアプライアンスの接続を可能にするためには、まず【*グローバル設定(Global Settings)*】ページでREDサポートを有効にする必要があります。

REDアプライアンスを追加するには、次の手順に従います。

1. **【*デバイス設定(Device Configuration)*】タブで、【*REDアプライアンスの追加(Add RED Appliance)*】をクリックします。**
   【*REDアプライアンスの追加(Add RED Appliance)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
ブランチ名(Branch Name): REDアプライアンスブランチの名前を入力します(例:「ミュンヘンオフィス」)。

RED ID: 設定しているREDアプライアンスのIDを入力します。このIDは、REDアプライアンスの背面とパッケージに記載されています。

ロック解除コード(Unlock Code)(オプション):REDアプライアンスの初回導入時にロック解除コードが生成されます。これはセキュリティ機能であり、REDアプライアンスを簡単に切断してどこにでもインストールできなくなります。設定中のREDアプライアンスを以前に導入したことがある場合は、ロック解除コードを指定する必要があります。(ロック解除コードを紛失した場合、REDアプライアンスをロック解除するためには、Astaroサポートに連絡してください。)

ASG ホスト名(Hostname):ASGがアクセスできるパブリックIPアドレスまたはホスト名を入力する必要があります。

アップリンクモード(Uplink Mode): REDアプライアンスがIPアドレスをどのように取得するのかを、DHCP経由またはスタティックIPアドレスの直接割り当てによって定義することができます。

- **DHCPクライアント(DHCP Client)**: REDはDHCP サーバからIPアドレスを取得します。
- **スタティックアドレス(Static Address)**: IPv4アドレス、関連するネットマスク、デフォルトゲートウェイ、DNSサーバを入力します。

オペレーションモード(Operation Mode): リモートネットワークをどのようにローカルネットワークに統合するのかを定義できます。

- **標準/統合(Standard/Unified)**:ASGがリモートネットワークのネットワークトラフィックを完全にコントロールします。さらに、DHCPサーバおよびデフォルトゲートウェイとして機能します。すべてのリモートネットワークはASG経由でルーティングされます。
- **標準/分割(Standard/Split)**:ASGがリモートネットワークのネットワークトラフィックを完全にコントロールします。さらに、DHCPサーバおよびデフォルトゲートウェイとして機能します。統合モードと違い、特定のトラフィックのみがASG経由でルーティングされます。下の【*分割ネットワーク(Split Networks)*】ボックスにローカルネットワークを定義します。このネットワークには、リモートクライアントからアクセス可能です。

- **透過/分割(Transparent/Split)**:ASGは、リモートネットワークのネットワークトラフィックをコントロールせず、DHCPとしてもデフォルトゲートウェイとしても機能しません。代わりに、リモートネットワークのDHCPサーバからIPアドレスを取得して、ネットワークの一部とします。ただし、リモートクライアントからローカルネットワークへのアクセスは有効化することができます。そのために、リモートネットワークによるアクセスを許可する*分割ネットワーク*を定義する必要があります。さらに、1つ以上の*分割ドメイン*をアクセス可能として定義することができます。ローカルドメインがパブリックに解決可能ではない場合、リモートクライアントからクエリ(問い合わせ)可能な*分割DNSサーバ*を定義する必要があります。

すべてのオペレーションモードの例は、【*導入ヘッダ(Deployment Helper)*】タブで参照できます。

注 - 次の設定は必ず手動で行ってください。1) 必要なファイアウォールルールの作成(【*ネットワークセキュリティ(Network Security)*】>>【*ファイアウォール(Firewall)*】>>【*ルール(Rules)*】)。2) 必要なマスカレーディングルールの作成(【*ネットワークセキュリティ(Network Security)*】>>【*NAT*】>>【*マスカレーディング(Masquerading)*】)。

3. ***【保存(Save)】*をクリックします。**
   REDアプライアンスの作成が行われ、ASGはAstaro RED Provisioning Service(RPS)に登録されます。

重要 - REDアプライアンスをRPSに登録した直後に、【*グローバル(Global)*】タブに指定したアドレスへEメールが送信されます(REDの有効化中)。このメールに記載された*ロック解除コード*は必ず保管しておいてください。このロック解除コードは、他のASGでREDアプライアンスを使用するときに必要になります。ロック解除コードが手元にない場合、REDアプライアンスをロック解除するためには、Astaroサポートに連絡する必要があります。

必要なファイアウォールルール(および、必要な場合はマスカレーディングルール)を設定したら、リモートサイトのREDアプライアンスをインターネットに接続することができます。ブート(起動)直後に、Astaro RED Provisioning Service(RPS)から設定が取得されます。その後、ASGとREDアプライアンス間の接続が確立されます。設定されたすべてのREDアプライアンスのステータスは、WebAdminの*RED*概要ページで確認できます。

REDアプライアンスの削除

REDアプライアンスを削除するには、アプライアンス名の横にある【*削除(Delete)*】ボタンをクリックします。
REDオブジェクトに依存関係があるという警告が表示されます。REDアプライアンスを削除して

も、関連するインタフェースと依存関係は*削除されません*。これは、REDアプライアンス間でインタフェースを移動できるようにするための意図的な設計です。

REDアプライアンスの設定を完全に削除するには、潜在的なインタフェースとその他の定義を手動で削除してください。

13.4導入ヘルパ

*【REDマネジメント(RED Management)】>>【導入ヘルパ(Deployment Helper)】*タブには、RED環境のセットアップと統合のためのウィザードがあります。このウィザードは、*【デバイス設定(Device Configuration)】*タブでの通常の設定の簡易版となります。必須フィールドと、必要に応じて「*オプション(optional)*」マークの付いたフィールドに入力して、*【REDの導入(Deploy RED)】*をクリックするだけです。

> **注 -** 利便性のため、「*標準/統合(Standard/Unified)*」および「*標準/分割(Standard/Split)*」モードでは、*【デバイス設定(Device Configuration)】*タブと違い、導入ヘルパが以下のオブジェクトを自動的に作成します。指定したIPアドレスのローカルインタフェース、利用可能なIPアドレス範囲の半分をカバーするリモートネットワーク用DHCPサーバ、ローカルDNSリゾルバへのアクセス。「*透過/分割(Transparent/Split)*」モードでは、導入ヘルパはDHCPクライアント(*ケーブルモデム(DHCP)*)インタフェースのみ作成します。

導入ヘルパは、各オプションについて概要を提供し、REDテクノロジーで提供される3つのオペレーションモードそれぞれについてスケッチを提供します。

以下は、REDの3つのオペレーションモードの説明と使用例です。

標準/統合(Standard/Unified)

ASGがリモートネットワーク全体を管理します。DHCPサーバおよびデフォルトゲートウェイとして機能します。
技術的には、REDアプライアンスのローカルインタフェースと、ローカルのASGへのアップリンクインタフェースは、このモードでブリッジされます。

例:支店が1つあり、セキュリティ上の理由から、そのすべてのトラフィックを本店のASG経由でルーティングしたい。これにより、リモートサイトは、LAN経由で接続されているようにローカルネットワークの一部となります。

標準／分割(Standard/Split)

「*標準/統合(Standard/Unified)*」モードと同様に、ASG がリモートネットワーク全体を管理します。DHCPサーバおよびデフォルトゲートウェイとして機能します。ただし、【*分割ネットワーク(Split Networks)*】ボックスにリストされたネットワーク宛てのトラフィックのみが、ローカルASGにリダイレクトされる点が異なります。
技術的には、REDアプライアンスのローカルインタフェースと、ローカルのASGへのアップリンクインタフェースは、このモードでブリッジされます。定義された分割ネットワークから発生していないすべてのトラフィックは、インターネットに直接ルーティングされます。

例:支店が1つあり、セキュリティ上の理由から、ローカルイントラネットへのアクセスを必要としているか、リモートネットワークのトラフィックをASG経由でルーティングしたい(例えば、トラフィックに対するウイルスチェックのため、あるいはHTTPプロキシを使用するため)。

透過／分割(Transparent/Split)

リモートネットワークは独立したままで、ASGはIPアドレスをリモートDHCP サーバから取得してこのネットワークの一部となります。リモートネットワークの特定のトラフィックのみ、特定のネットワークまたはローカルドメインへのアクセスが許可されます。ASGはリモートネットワークをコントロールできないため、*分割DNSサーバ*を定義しない限り、パブリックに解決可能ではないローカルドメインをリモートルータで解決することはできません。これは、リモートクライアントからクエリ(問い合わせ)可能なローカルDNSサーバです。

技術的には、REDアプライアンスのローカルインタフェースと、ローカルのASGへのアップリンクインタフェース、並びにリモートルータへのリンクは、このモードでブリッジされます。ASGはリモートネットワークの唯一のクライアントであるため、分割ネットワークへのトラフィックを他のモードと同様にルーティングすることはできません。そのため、REDアプライアンスはすべてのトラフィックをインターセプトします。【*分割ネットワーク(Split Networks)*】ボックスにリストされたネットワーク宛てのトラフィックや、【*分割ドメイン(Split Domains)*】ボックスにリストされたドメイン宛てのトラフィックは、ASGインタフェースにリダイレクトされます。これは、各データパケット内でデフォルトゲートウェイのMACアドレスをASGのMACアドレスに置き換えることで実現します。

例:イントラネットや、ローカルネットワーク内の特定のサーバへのアクセスが必要なパートナーまたはサービスプロバイダがいる。REDアプライアンスを使用することで、このパートナーのネットワークは自社のネットワークからの独立が完全に保たれますが、特定の目的のために、自社のネットワークの決められた部分にLAN経由で接続しているかのようにアクセスすることはできます。

注 - 導入ヘルパを使用すると、REDアプライアンスのアップリンクモードはいずれのオペレーションモードでも*DHCPクライアント*となります。代わりにスタティックIPアドレスを割り当てる必要がある場合は、【*デバイス設定(Device Configuration)*】タブでREDアプライアンスを設定する必要があります。

14ログ管理

Astaroログ管理は、ネットワークの内外にあるさまざまなデバイスからのログファイルを単一の管理インタフェースで処理する汎用ユーティリティです。どこからでも迅速にログを確認でき、使いやすい検索機能を利用してすべてのログファイルから一度に検索することが可能です。

さらに、事前定義されたルールセットにより、何か重要なイベントが発生するとすぐに通知が送られます。必要に応じてこれらのルールを変更したり、新しいルールを作成することができます。

ログ管理には、ログファイルに関する多様なレポーティング機能があり、情報がシンプルかつクリアに保たれます。

ログ管理アルゴリズムはログファイルからの学習により、通常のログと異常なログを見分けることが可能になります。

ログ管理はクラウドベースのアプリケーションです。設定されたすべてのデバイスが、暗号化形式でレポートをアプリケーションに送ります(証明書認証付きのTLS)。ログ管理用アカウントはサブスクリプションIDで識別され、Joinコードによって保護されます。ログ管理インスタンスへのレポートが必要なすべてのデバイスは、これらのクレデンシャルを使用して設定する必要があります。Astaro Security Gatewayとログ管理インスタンスの間の通信は、ポート5000～5200で行われます。ASGが実際に使用するポートは、ログ管理を有効にすると生成されます。

この章には次のトピックが含まれます。

- 概要
- ログ管理インタフェース
- ログ転送
- デバイス設定

14.1概要

【ログ管理(Log Management)】>>*【概要(Overview)】*ページでは、ASGのログ管理を有効にできます。ログ管理が無効になっている場合(デフォルト)、【概要(Overview)】ページにはログ管理、セットアップスケッチ、および詳細情報の場所などに関する基本情報が表示されます。

ASGのログ管理を有効にするには、以下の手順に従います。

1. ***【概要(Overview)】*タブで、ログ管理を有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

ステータスアイコンがアンバー色になり、いくつかの設定フィールドが表示されます。

ログ管理を初めて有効にしたときは、最初のオプションが有効化されています。

2. **状況に応じて適切なオプションを選択します。**
   - 初回有効化(First activation):過去にASGを有効化したことがない場合、最初のオプションを選択します。
     必須フィールドに入力します。
   - 再有効化(Re-activation):ログ管理を再び有効化する場合や、ASGのレポート先を既存のログ管理インスタンスにする場合には、2番目のオプションを選択します。
     ASGを過去に有効化していた場合、【*アカウントID(Account ID)*】および【*Joinコード(Join Code)*】には既にログイン用資格情報が記入されています。既存のログ管理インスタンスへレポーティングさせる場合は、このインスタンス用のアカウントIDとJoinコードをここに入力します。
3. **利用条件への同意を示します。**
   利用条件には必ず同意する必要があります。説明のリンクをクリックし、読んでください。
4. **【*有効化(Enable)*】をクリックします。**
   数秒後にステータスアイコンが緑色になり、ログ管理が有効になります。サブスクリプションIDおよびJoinと、Web上の管理インタフェースにログインするための【*ログイン(Login)*】ボタンが表示されます。

ログ管理が有効である場合、ASGはポート443でプロビジョニングサービスを利用します。その後、【*概要(Overview)*】ページで指定したホストとポートを使用してクラウドサービスにログファイルを送信する必要があります。したがって、ASGとインターネットの間に別のファイアウォールが存在する場合、プロビジョニングサービスおよびクラウドサービスとの通信を有効にするために、このファイアウォール上にパケットフィルタルールを作成する必要があります。

ログ管理を再び無効にするには、ステータスバーまたは【*無効(Disable)*】ボタンをクリックします。無効化しても、再び必要になった場合のためにログ管理用資格情報は保持されます。ログ管理を再有効化すると、この資格情報が表示されます。

14.2ログ管理インタフェース

Astaroのログ管理はクラウドベースのアプリケーションなので、Webブラウザ経由でアクセスする必要があります。【*概要(Overview)*】タブのログインボタンをクリックするか、URLを手動で入力することができます(【*デバイス設定(Device Configuration)*】タブに表示されます)。

Astaroログ管理をWebAdminなどから起動すると、ダッシュボードが表示されます。ここには、最新のログファイルが表示されています。

ログ管理インタフェースは以下のメニューを使用して管理します。メニューについては次のセクションで詳しく説明します。

- ダッシュボード(Dashboard):最新のログアクティビティ、ログ検索、および関係ブラウザ
- グラフ(Charts):ログ量がグラフ形式で表示されます。
- イベント(Events):重要度に従って色分けされたログイベント
- デバイス(Devices):デバイス別のログ。デバイスを管理します。
- 設定(Settings):ルール、アカウント設定、adminアカウント、Windows Agent(未公開)
- レポート(Reports):さまざまな時間範囲に対するレポートを作成します。
- ヘルプ(Help):『はじめに(Getting Started Guide)』を表示します。
- ログアウト(Logout):Astaroログ管理からサインアウトします。
- 検索(Search):すべてのログファイルを対象に検索を開始します。

14.2.1ダッシュボード

ダッシュボードは、ログイベントをテキストで表示する*イベントタイムライン*と、*ログ量*の増減を経時的に示す下部のエリアから構成されています。

イベントタイムライン

イベントタイムラインは、最新のログイベントをグラフィカルに表示します。主に2つのタイムラインがあります。上部のグレーのタイムラインは日単位を示し、下部の白いタイムラインはログイベントを、1日に占める時間で示します。いずれのタイムラインとも、左や右に動かして、過去や未来に移動することができます。

日単位のタイムラインには、ログイベントが小さい青いストライプとして表示されます。ストライプが多かったり、幅広い場合は、ログイベントが多いことを示します。

時間タイムラインの1つのログイベントには、複数のログファイルが含まれる場合があります。これは、複数の類似ログファイルが短時間で発生した場合などです。ログイベントをクリックすると、イベント詳細のウィンドウが開きます。このイベント詳細ウィンドウについては、「イベント」のセクションを参照してください。

ログイベントは色分けされており、重要なイベントを簡単に見分けることができます。

- 赤: 重大度が高いイベント
- 黄色: 重大度が中程度のイベント
- 緑色: 重大度が低いイベント

注 - イベントタイムラインは、最重要イベントの概要を知るためのものです。短時間に多くのイベントが発生した場合に、すべてのイベントを確認するためには、【イベント(Events)】ページを閲覧する必要があります。

さらに、ログ管理エンジンは、頻度の少ないイベント(*レア(Rare)*)と増加したイベント(*増加(Incr.)*)を識別します。これはすべてのデバイスを対象に、通常のログ動作からの差異を示す補足情報です。エンジンの背後にあるアルゴリズムでは、すべてのログから情報を収集するため、このような情報は時間の経過とともに信頼性が向上します。

ログ量

ログ量タイムラインは、ログファイルの量の増減をグラフで表示します。このグラフは、ログの異常な増加を一目で検出するために使用します。白い点を1つクリックすると、【グラフ(Charts)】セクションにリダイレクトします。

ログの検索[Log Search]

【ダッシュボード(Dashboard)】メニューには検索機能もあります。*【ダッシュボード(Dashboard)】>【ログ検索(Log Search)】*メニューをクリックして開きます。

【ログ検索(Log Search)】ページを開くと、過去24時間のログファイルが表示されます。上部には検索バーがあり、検索対象とする時間範囲と1つ以上のキーワードを指定できます。*【検索(Search)】*ボタンをクリックして検索を開始します。

*【エクスポート(Export)】*ボタンをクリックして、検索結果をエクスポートすることもできます。選択できるエクスポート形式はJSONまたはXMLです。

結果テーブルには、検索結果が時間順に表示され、ログファイルの発生源となったデバイスとプログラム、ログレベル、ログメッセージなどの情報を確認できます。

左側のサイドバーにあるドロワを使用して、デバイス、ログレベル、プログラムを基準に検索結果をさらにドリルダウンできます。これを行うには、ドロワのヘッダをクリックし、ドロワエントリが複数あればいずれかを選択します。ドロワのヘッダには、それぞれ2つのアイコンがあります。

- **+/-**: クリックすると、そのドロワが開閉します。ドロワは、ドロワのヘッダの任意の場所をクリックしても開閉可能です。

- **ギア**: ギアをクリックすると、ドロワエントリ選択の逆の結果を表示するか(【*逆を選択(Select Inverse)*】)、すべてのエントリを選択(【*すべてを選択(Select All)*】)することができます。

ヒント - サイドバーは、サイドバーとテーブルの境界の中央にある小さい矢印アイコンを使用して閉じることができます。サイドバーを閉じると、矢印アイコンはテーブルの左境界の中央に表示され、クリックするとサイドバーがもう一度開きます。

関係ブラウザ(Relation Browser)

【ダッシュボード(Dashboard)】メニューには関係ブラウザもあります。【*ダッシュボード(Dashboard)*】>【*関係ブラウザ(Relation Browser)*】メニューをクリックして開きます。

関係ブラウザは、最重要イベントの間のナビゲート関係をグラフィカルに表示します。トップのデバイスから順に表示されます。つまり、過去24時間で最も多くのイベントを報告したデバイスです。

いずれかのデバイスをクリックすると、調査を開始できます。関係ブラウザには、上位10イベントがデバイスの優先順位に従って表示されます。イベントをクリックすると、このイベントに関する詳細情報(IPアドレスまたはユーザ名、変数など)が表示されます。ユーザ名、IPアドレス、または変数をクリックすると、これに関連付けられた他のログイベントが表示されます。これにより、イベント間の関係やシステム間で行われた動作を特定することができます。

14.2.2グラフ

Astaroログ管理の【*グラフ(Charts)*】ページは、特定の時間枠内のログ量をグラフィカルに表示します。このページは、ドロワのあるサイドバーと、グラフを表示するメインエリアに分かれています。

日付(Date): グラフのヘッダには、このグラフの対象時間枠が表示されます("2011 July 19"など)。年をクリックすると、その年全体のグラフが表示され、月をクリックすると、その月全体のグラフが表示されます。

前へ(Previous)/次へ(Next): 日付の左右にあるボタンを使用して、定義した時間範囲で過去や未来に移動することができます。

例1: 現在の時間範囲が"2011 July 19"であるときに【*前へ(Previous)*】をクリックすると、日付が"2011 July 18"に遡ります。

例2: 現在の時間範囲が"2011 July 19 2:00"であるときに【*前へ(Previous)*】をクリックすると、日付が"2011 July 19 1:00"に遡ります。

ログメッセージの閲覧(View Log Messages): このボタンをクリックすると、現在の時間範囲に対するすべてのログメッセージが表示されます。

14.2.3イベント

ログ管理の【*イベント(Events)*】ページは、タイムラインまたはリストでログイベントを表示します。さらに、タイムラインをフィルタするためのサイドバーもあります(詳しくは後述)。

タイムライン

タイムラインは、ダッシュボードのタイムラインと同様に機能します。ただし、月単位のタイムラインが追加されています。

リスト

リストには、過去24時間から順にすべてのログイベントが表示されます。重大度、所有者、ステータス、説明などの情報が表示されます。下にあるバーを使用して、すべてのログイベントを参照したり、新しいログイベントがもたらされた場合にビューを更新することができます。

サイドバー

サイドバーにはドロワがあり、タイムラインまたはリストに表示された結果をフィルタするために使用できます。これを行うには、ドロワのヘッダをクリックし、ドロワエントリが複数あればいずれかを選択します。ドロワのヘッダには、それぞれ2つのアイコンがあります。

- **+/-**: クリックすると、そのドロワが開閉します。ドロワは、ドロワのヘッダの任意の場所をクリックしても開閉可能です。
- **ギア(Gear)**: ギアをクリックすると、ドロワエントリ選択の逆の結果を表示するか(【*逆を選択(Select Inverse)*】)、すべてのエントリを選択(【*すべてを選択(Select All)*】)することができます。

ヒント - サイドバーは、サイドバーとテーブルの境界の中央にある小さい矢印アイコンを使用して閉じることができます。サイドバーを閉じると、矢印アイコンはテーブルの左境界の中央に表示され、クリックするとサイドバーがもう一度開きます。

1つのドロワに1つ以上のエントリが含まれる場合があり、適用されるログイベントの数が数字で示されます。例 : *重大度*のドロワには「*Low 712*」というエントリが含まれており、重大度がLowのイベントが712件あることを示します。エントリをクリックすると、これら712件のログイベントだけが表示されるようになります。

デバイス(Devices): ログ管理にログファイルを送信するすべてのデバイスが表示されます。

重大度(Severity): ログイベントの重大度(*低(Low)*、*中(Medium)*、または*高(High)*)が表示されます。

ステータス(Status): ワークフローに関連します。ログファイルのステータスは、*新規(New)*、*受入済(Accepted)*、または*終了(Closed)*のいずれかです。

所有者(Owner): ワークフローに関連します。「*なし(None)*」には、ユーザが受け入れたか終了させたすべてのログイベントが含まれます。

ルール(Rule): ログイベントによって有効化されたルールを表示します。

イベントの詳細

ログイベントをクリックすると、別ウィンドウが開き、ログイベントのID、説明、作成日、重大度レベル、ステータス、含まれるログ数などの詳細情報が表示されます。10分間で同じタイプのログが複数件作成された場合は、1つのログイベントに複数のログが含まれる場合があります。

イベント詳細のウィンドウの下部にある【*ログ(Logs)*】タブには、このイベントに属するすべてのログファイルが表示されます。

ワークフロー(Workflow): ログイベントはデフォルトでワークフローの一部です。ただし、ログ管理でワークフロー機能を使用するのはオプションです。この機能を使用してイベントログをトラッキングし、(重要な)ログイベントを見落としていないことを確認できます。ログイベントのステータスは、任意のユーザが受け入れるか終了させるまで「*新規(New)*」のままとなります。
ログイベントを受け入れるか終了させるには、ウィンドウの上部にある【*ワークフローの更新(Update Workflow)*】フィールドを使用します。オプションで、フィールドにコメントを入力することができます。【*ワークフロー(Workflow)*】タブには、ログイベントの現在のワークフローステータスが表示されます。

14.2.4デバイス

ログ管理の【*デバイス(Devices)*】ページは、ログ管理に対して現在ログファイルを送信しているデバイスまたは過去にログファイルを送信したデバイスを表示します。

テーブルには、デバイスに関する以下の情報が表示されます。

- **エイリアス(Alias)**: デフォルトではデバイスのホスト名です。ただし、ログ管理インタフェース全体でデバイスを簡単に識別できるように、エイリアスを変更することができます。
- **ホスト名(Hostname)**: デバイスのホスト名。
- **初回検出(First Seen)**: あるデバイスがロギングデータを初めて送信したのがいつかを表示します。

- **最終検出(Last Seen)**: あるデバイスがロギングデータを最後に送信したのがいつかを表示します。
- **タイムオフセット(Time Offset)**: ここでは、複数のタイムゾーンに対応するために、タイムオフセットを調整できます。
- **有効(Enabled)**: ログファイルの送信がデバイスで有効化されているかどうかを示します。デバイスを無効にしたい場合、このデバイスの行を右クリックし、コンテキストメニューから【*デバイスの無効化(Disable Device)*】を選択します。デフォルトで、無効化されたデバイスはテーブルに表示されなくなります。これらも表示するには、テーブルの上にある【*無効を表示(Show Disabled)*】ボタンをクリックします。

14.2.5設定

ログ管理の【*設定(Settings)*】メニューには、*ルール(Rules)*、*アカウント設定(Account Settings)*、*Adminアカウント(Admin Accounts)*という各設定があります。

ルール(Rules)

Astaroログ管理には、各種ロギングデバイス用に事前定義されたルールセットが用意されています。ルールにより、特定のタイプのログイベントが発生したときにどのようなアクションをとるべきかを定義します。【*設定(Settings)*】>【*ルール(Rules)*】ページで、必要に応じて事前定義されたルールに変更を加えたり、追加のルールを作成することができます。

【*ルール(Rules)*】テーブルには、ルールの説明、ルールに属するイベントの重大度レベルの分類、アラート発生の有無、ルールが有効か無効かといった情報が表示されます。

【*ルール(Rules)*】ページの一番上には、次の機能があります。

- **新規(New)**: このボタンをクリックして、新しいルールを作成します。
- **削除(Delete)**: このボタンをクリックして、ルールを削除します。ルールは削除せずに無効にすることもできます。
- **有効化(Enable)**: このボタンをクリックして、ルールを再有効化します。
- **無効化(Disable)**: このボタンをクリックして、ルールを無効にします。つまり、ルールはアクティブでなくなります。

ヒント -`Ctrl`キーを押したままルールをクリックして、複数のルールを選択することができます。

- **エクスポート(Export)**: このボタンをクリックして、現在のビューをXMLにエクスポートします。

- **インポート(Import)**: このボタンをクリックして、新しいルールのセットをインポートできます。これにより、ルールを手動で作成する必要がなくなります。
- **検索(Search)**: 検索ボックスを使用して、1つ以上のキーワードでルールを検索します。【*検索(Search)*】ボタンをクリックしてトピックを選び、検索エリアを制限することができます。

ルールの作成または変更

既存のルールを変更したり、新規ルールを作成できます。ルールの変更は、ルールの新規作成と非常に似ているため、ここではルールの新規作成についてのみ説明します。

新しいルールを作成するには、次の手順に従います。

1. ***【ルール(Rules)】ページの一番上で、【新規(New)】をクリックします。***
   【*新規ルール(New Rule)*】ダイアログウィンドウが開きます。
2. ***【詳細(Details)】タブで、次の設定を行います。***
   名前(Name): ルールを説明する名前を入力します。

   説明(Description): ルールの説明を入力します。

   有効(Enabled): ルールはデフォルトで有効化されています。チェックボックスのチェックを外すと、ルールが無効になります。

   イベントの重大度(Event Severity): このルールのログイベントをどのように分類すべきかを定義します。
3. ***【条件(Conditions)】タブで、次の設定を行います。***
   ルールを起動する条件を定義する必要があります。条件を作成するには、ドロップダウンフィールドを使用します。【*追加(Add)*】ボタンをクリックして他の条件を追加し、【*削除(Delete)*】ボタンをクリックして条件を削除します。

   演算子(Operator): ANDまたはOR演算子を使用して、複数のルールを論理的に組み合わせることができます。
4. ***【アラート(Alerts)】タブで、通知を受け取るかどうか決定します。***
   デフォルトでは、アラートはオフになっています。ルールが起動したときに通知を受け取りたい場合は、チェックボックスにチェックを入れます。
5. ***【送信(Submit)】をクリックしてルールを保存します。***
   ルールが保存され、【*ルール(Rules)*】テーブルに表示されます。

既存のルールを変更するには、【*ルール(Rules)*】テーブルでルールをダブルクリックします。

アカウント設定(Account Settings)

【*設定(Settings)*】>【*アカウント設定(Account Settings)*】をクリックすると、【*アカウント設定(Account Settings)*】ダイアログウィンドウが開きます。このダイアログウィンドウを使用して、ログイン名、Eメールアドレス、パスワードを変更することができます。さらに、アニメーションを無効または有効にしたり、マネージャレポートを受け取るか否か(受け取るならそのタイミング)を選択することができます。

Adminアカウント(Admin Accounts)

【*設定(Settings)*】>【*Adminアカウント(Admin Accounts)*】ページでは、管理権限あり(またはなし)で新規ユーザを作成し、管理することができます。管理権限なしのユーザは、他のユーザのアカウントを作成したり管理することはできません。

新しいユーザを作成するには、次の手順に従います。

1. **【*アカウント(Accounts)*】ページの一番上で、【*新規(New)*】ボタンをクリックします。**
   【*新規アカウント(New Account)*】ダイアログウィンドウが開きます。
2. **次の設定を行います。**
   ログイン名(Login Name): ユーザがログ管理インタフェースへのログインに使用する名前を入力します。

   Eメールアドレス(Email): ユーザのEメールアドレスを入力します。このアドレスに、レポートおよび通知のEメールが送信されます。

   パスワード(Password): ユーザのパスワードを入力し、確認のためにもう一度入力します。6文字以上にする必要があります。

   Admin: ユーザにAdmin権限を付与する場合は、このチェックボックスにチェックを入れます。
3. **【*送信(Submit)*】をクリックして新しいアカウントを保存します。**
   新しいアカウントが保存され、【*アカウント(Accounts)*】テーブルに表示されます。

ユーザを削除するには、【*アカウント(Accounts)*】ページの上部にある【*削除(Delete)*】ボタンをクリックします。

14.2.6レポート

ログ管理は、サブスクライブしている各ユーザの最新のアクティビティに関する概要レポートを毎週送信します(この設定は、各ユーザが【*アカウント設定(Account Settings)*】ウィンドウで変更で

きます)。ウィークリーレポートとは別に、ログ管理の【*レポート(Reports)*】ページで個別にレポートを生成することができます。このようなマネージャレポートは、過去の週に対して事前定義されたレポートを選択するか、下のフィールドで特定の日付を選択して簡単に生成することができます。選択した日付は、1週間というレポート期間の終了日となります。

注 - レポートの参照にはAdobeビューアが必要です。

14.3ログ転送

ログ管理は、ネットワーク内またはASGの背後にあるデバイスでも使用できます。【*ログ管理(Log Management)*】>>【*ログ転送(Log Forwarding)*】ページでは、他のデバイスからのログファイルも受け入れるようにASGを設定することができます。これにより、ASGは暗号化されていないsyslogメッセージを受信してからこれを暗号化し、お使いのログ管理インスタンスに送信するようになります。

ログ転送を有効にするには、次の手順に従います。

1. **【*ログ転送(Log Forwarding)*】タブで、ログ転送を有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色になり、2つの設定フィールドが表示されます。

2. **次の設定を行います。**
   許可ネットワーク(Allowed Networks): 対象のデバイスが存在しており、ASGへのログ送信を可能にする必要があるネットワークを選択または追加します。

   ログ転送用ASGポート(ASG Port for Log Forwarding): 暗号化されたログファイルをログ管理インスタンスに送信するために使用するポート。デフォルトのポートは`10101`です。必要に応じてポート番号を変更できますが、一部のポートは他のサービス用に予約されています。

3. **【*適用(Apply)*】をクリックします。**

   ステータスアイコンが緑色になり、ログ転送が有効になります。

14.4デバイス設定

【*ログ管理(Log Management)*】>>【*デバイス設定(Device Configuration)*】ページは、ログ管理で使用する複数のデバイスの設定方法に関する情報を提供します。

また、ログ管理についての『はじめに(Getting Started Guide)』(http://www.astaro.com/lm)もあります。

15サイト間VPN

この章では当製品のサイト間VPN設定の構成方法について説明します。Astaro Security Gateway.Astaro Security Gatewayのサイト間VPNは、*バーチャルプライベートネットワーク(Virtual Private Networks)*(VPN)によって実現します。VPNはインターネットなどの公共のネットワーク上でリモートネットワークが極秘に相互通信するためのセキュアでコスト効果の高い方法です。VPNでは暗号化トンネリングプロトコルのIPsecを使用して、VPN上を伝送されるデータの機密性とプライバシを保ちます。

クロスリファレンス - サイト間VPN接続の設定方法の詳細は、Astaroナレッジベースを参照してください(「*ASG バージョン7*」>>「*Astaroマニュアルおよびガイド*」の順にアクセスします)。

この章には次のトピックが含まれます。

- IPsec
- SSL
- 証明書管理

WebAdminの【*サイト間VPN(Site-to-site VPN)*】概要ページには、設定されたすべてのIPsecおよびSSL接続とその現在のステータスが表示されます。各接続の状態は、そのステータスアイコンの色で示されます。ステータスアイコンは2種類あります。接続名の隣りの大きなアイコンは、接続の全体的な状態を表します。それぞれの色は以下の状態を意味します。

- 緑色 – すべてのSA(*セキュリティアソシエーション*)が確立されました。接続は完全に機能しています。
- 黄色 – SAの一部が確立されていません。接続は部分的に機能しています。
- 赤色 - SAがまったく確立されていません。接続が機能していません。

トンネル情報の隣りの小さなアイコンは、トンネルの状態を表します。それぞれの色は以下の状態を意味します。

- 緑色 – すべてのSAが確立されました。トンネルは完全に機能しています。
- 黄色 – IPsec SAが確立されましたが、ISAKMP SA(*インターネットセキュリティアソシエーションと鍵管理プロトコル*)が機能していません。トンネルは完全に機能しています。
- 赤色 - SAがまったく確立されていません。接続が機能していません。

15.1IPsec

IPsec(IP Security)とは、すべてのIPパケットを暗号化または認証すること(あるいはその両方)によってIP(*インターネットプロトコル*)通信のセキュリティを維持するための標準です。

IPsec標準は、次の2つのサービスモードと2つのプロトコルを定義しています。

- トランスポートモード
- トンネルモード
- *AH*(認証ヘッダ)認証プロトコル
- *ESP*(カプセル化セキュリティペイロード)暗号化(および認証)プロトコル

IPsecには、SA(*セキュリティアソシエーション*)と鍵配布を手動および自動で管理するための方法も用意されています。これらの特徴は、DOI(*解釈ドメイン*)で一元管理されています。

IPsecモード

IPsecは、トランスポートモードまたはトンネルモードで機能します。原則的に、ホスト間接続ではどちらのモードも使用できます。ただし、いずれかのエンドポイントがセキュリティゲートウェイである場合、トンネルモードを使用する必要があります。このASGでのIPsec VPN接続では、常にトンネルモードが使用されます。

トランスポートモードでは、元のIPパケットは他のパケットにカプセル化されません。元のIPヘッダは維持され、パケットの残りの部分は平文のまま(AH)またはカプセル化されて(ESP)送信されます。パケット全体をAHで認証することも、ESPでペイロードをカプセル化して認証することもできます。いずれの場合も、元のヘッダは平文としてWAN経由で送信されます。

トンネルモードでは、パケットヘッダとペイロードの全体が新しいIPパケットにカプセル化されます。IPヘッダがIPパケットに追加され、宛先アドレスは受信側トンネルエンドポイントに設定されます。カプセル化パケットのIPアドレスは変更なしで維持されます。続いて、元のパケットがAHで認証されるか、ESPでカプセル化されて認証されます。

IPsecプロトコル

IPsecでは、IPレベルで安全に通信するために2つのプロトコルを使用します。

- **AH(認証ヘッダ)**:パケット送信者を認証し、パケットデータの完全性を保証するためのプロトコル。
- **ESP(カプセル化セキュリティペイロード)**:パケット全体を暗号化し、そのコンテンツを認証するためのプロトコル。

AH(認証ヘッダ)プロトコルは、パケットデータの信頼性と完全性をチェックします。さらに、送信者と受信者のIPアドレスが送信中に変更されていないことをチェックします。パケットは、ハッシュベースのメッセージ認証コード(HMAC)と鍵を使用して作成されたチェックサムを使用して認証されます。次のいずれかのハッシュアルゴリズムが使用されます。

- **MD5(メッセージダイジェスト、バージョン5)**:このアルゴリズムでは、任意のサイズのメッセージから128ビットのチェックサムが生成されます。このチェックサムはメッセージの指紋のようなもので、メッセージが変更されるとチェックサムも変わります。このハッシュ値は、デジタル署名またはメッセージダイジェストとも呼ばれます。
- **SHA-1(セキュアハッシュ)**:このアルゴリズムではMD5と類似したハッシュが生成されますが、SHA-1ハッシュは長さが160ビットです。SHA-1は鍵がMD5より長いため、MD5より強力なセキュリティが実現します。

MD5と比較すると、SHA-1ハッシュは計算が難しく、生成に必要なCPU時間はより長くなります。もちろん、計算速度は、プロセッサの処理速度とAstaro Security Gatewayで使用されるIPsec VPN接続の数に依存します。

ESP(カプセル化セキュリティペイロード)プロトコルには、暗号化以外に、送信者を認証し、パケットコンテンツを検証する機能もあります。トンネルモードでESPを使用すると、IPパケット全体(ヘッダとペイロード)が暗号化されます。ここで、暗号化されていないIPヘッダとESPヘッダがカプセル化するパケットに追加されます。新しいIPヘッダには、受信側ゲートウェイと送信側ゲートウェイのアドレスが含まれています。これらのIPアドレスは、VPNトンネルのアドレスです。

暗号化付きのESPでは、通常次のアルゴリズムが使用されます。

- 3DES(トリプルデータ暗号化標準)
- AES(高度暗号化標準)

これらのうち、AESが最も安全です。AESで使用可能な鍵の有効長は128ビット、192ビット、256ビットです。Astaro Security Gateway は、多数の暗号化アルゴリズムをサポートしています。認証にはMD5またはSHA-1アルゴリズムを使用できます。

NAT-T(NATトラバーサル)

NAT トラバーサルとは、NATデバイスを使用するTCP/IPネットワーク内のホスト間で接続を確立するための技術です。この接続は、ESPパケットのUDPカプセル化を使用して、NATデバイス経由でIPsecトンネルを確立することによって実現します。UDPカプセル化は、IPsecピア間でNATが検出された場合のみに使用されます。検出されなかった場合は、通常のESPパケットが使用されます。

NATトラバーサルにより、ゲートウェイまたはロードウォリアをNATルータの背後に配置しながら、IPsecトンネルを確立できるようになります。この機能を使用する場合、両方のIPsecピアでNATトラバーサルがサポートされている必要があります。ネゴシエーションは自動的に行われます。NATデバイスでIPseパススルーがオフになっていることを確認してください。オンになっていると、NATトラバーサルの使用に支障が出る可能性があります。

ロードウォリアでNATトラバーサルを使用したい場合、WebAdmin内の対応ユーザオブジェクトにスタティックリモートアクセスIPアドレス(RAS アドレス)が設定されている必要があります(WebAdminのユーザ定義 ページで【*スタティックリモートアクセスIPを使用(Use Static Remote Access IP)*】も参照してください)。

データ未送信時に確立されたトンネルが期限切れになることを防ぐために、NATトラバーサルのkeep-alive信号がデフォルトで60秒間隔で送信されます。keep-aliveメッセージは、NATルータがセッションに関連するステート情報を維持しており、トンネルが開いたままであることを確認するために送信されます。

TOS

「サービスタイプ」ビット(TOSビット)は、IPヘッダにあるいくつかの4ビットフラグです。これらのビットは、どのタイプのサービス品質が必要であるかを転送アプリケーションがネットワークに伝えることを許可するため、*サービススタイプビット*と呼ばれています。

Astaro Security GatewayへのIPsec導入では、TOSの値は常にコピーされます。

15.1.1接続

*【サイト間VPN(Site-to-site VPN)】>>【IPsec】>>【コネクション(Connections)】*タブでは、IPsec接続を作成および編集することができます。

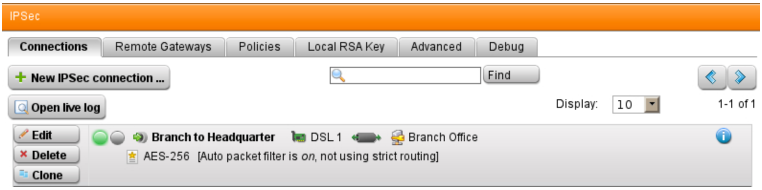


図130 サイト間VPN IPsec:接続リスト

IPsecコネクションを作成するには、次の手順に従います。

1. ***【コネクション(Connections)】タブで、【新規IPsecコネクション(New IPsec Connection)】をクリックします。***
   *【IPsecコネクションの追加(Add IPsec Connection)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): このコネクションを説明する名前を入力してください。

   リモートゲートウェイ(Remote Gateway): リモートゲートウェイ定義を選択します。リモートゲートウェイは、*【サイト間VPN(Site-to-site VPN)】>>【IPsec】>>【リモートゲートウェイ(Remote Gateways)】*タブで設定します。

   ローカルインタフェース(Local Interface): IPsecトンネルのローカルエンドポイントとして使用されるインタフェースの名前を選択します。

   ポリシ(Policy): このIPsecコネクションのIPsecポリシを選択します。IPsecポリシは、*【サイト間VPN(Site-to-site VPN)】>>【IPsec】>>【ポリシ(Policies)】*タブで定義できます。

   ローカルネットワーク(Local Networks): VPNトンネル経由でアクセス可能にするローカルネットワークを選択します。

   自動ファイアウォールルール(Auto Firewall Rules): このオプションを選択すると、VPN接続用のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、VPN接続の確立が成功するとすぐに追加され、VPN接続が切断されると削除されます。より厳格なIPsec接続を使用する場合は、*【自動ファイアウォールルール(Auto Firewall Rules)】*を使用しないで、代わりにファイアウォールルールセット内のIPsecオブジェクトを使用します。

   ストリクトルーティング(Strict Routing): ストリクトルーティングを選択すると、VPNルーティングは(宛先IPアドレスのみではなく)送信元IPアドレスと宛先IPアドレスに従って実行されます。この場合、VPNトンネル定義と完全に一致するパケットのみがVPNトンネルにルーティングされます。この結果、SNATを使用して本来トンネル定義の一部ではないネット

ワークまたはホストをVPNトンネルに追加することはできません。一方、ストリクトルーティングを使用しない場合、異なる送信元アドレスから同じネットワークに対して非暗号化/暗号化の混在するセットアップを行うことはできません。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
新しい接続がIPsecの*【接続(Connections)】*リストに表示されます。

接続を編集または削除するには、対応するボタンをクリックします。

ライブログを開く(Open Live Log): IPsec VPNライブログには、確立されたIPsec接続に関するモニタリング情報が表示されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

15.1.2リモートゲートウェイ

*【サイト間VPN(Site-to-site VPN)】>>【IPsec】>>【リモートゲートウェイ(Remote Gateways)】*タブでは、サイト間VPNトンネル用にリモートゲートウェイを定義できます。これらのリモートネットワーク定義は、*【IPsec】>>【接続(Connections)】*タブでIPsec接続を作成すると使用可能になります。

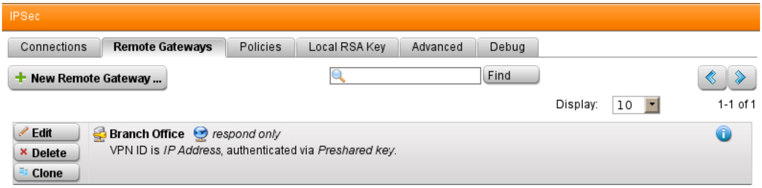


図131 サイト間VPN IPsec:リモートゲートウェイリスト

リモートゲートウェイを追加するには、次の手順に従ってください。

1. ***【リモートゲートウェイ(Remote Gateways)】タブで、【新規リモートゲートウェイ(New Remote Gateway)】をクリックします。***
*【リモートゲートウェイの追加(Add Remote Gateway)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
名前(Name): このリモートゲートウェイを説明する名前を入力してください。

ゲートウェイタイプ(Gateway Type): ゲートウェイのタイプを選択します。次のタイプを使用できます。

- **接続の初期化(Initiate Connection)**: リモートエンドポイントにスタティック(静的)IPアドレスがあり、リモートゲートウェイへの接続をゲートウェイによって開始できる場合に選択します。選択する場合、【*ゲートウェイ(Gateway)*】ボックスにリモートゲートウェイを指定します。このオプションは、リモートゲートウェイがDynDNSによって解決される場合にも選択できます。

- **応答のみ(Respond Only)**: リモートエンドポイントのIPアドレスが不明であるか、DynDNSで解決できない場合に選択します。ゲートウェイはリモートゲートウェイへの接続を開始できず、応答のみを必要とする接続を受信するまで待機します。

認証タイプ(Authentication Type): このリモートゲートウェイ定義の認証タイプを選択します。次のタイプを使用できます。

- **事前共有鍵(Preshared key)**: *事前共有鍵*(PSK)による認証では、秘密のパスワードを鍵として使用します。これらのパスワードは、接続を確立する前にエンドポイントに配布する必要があります。新しいVPNトンネルが確立されると、両端で、相手側が秘密のパスワードを知っていることのチェックが行われます。PSKのセキュリティは、使用するパスワードの品質に依存します。一般的な言葉や成句では、辞書攻撃に対して脆弱です。常時のIPsec接続や長期的なIPsec接続では、パスワードの代わりに証明書またはRSA鍵を使用する必要があります。

- **RSA鍵(RSA Key)**:RSA鍵を使用する認証は、より高度です。この方式では、公開鍵と秘密鍵から成る鍵ペアが接続の両端で生成されます。秘密鍵は、鍵交換時の暗号化と認証で必要です。この認証方式を使用するIPsecVPN接続の両エンドポイントは、独自の鍵ペアを必要とします。リモートユニットの公開RSA鍵(【*サイト間VPN(Site-to-site VPN)*】>>【*IPsec*】>>【*ローカルRSA鍵(Local RSA Key)*】)をローカルユニットの【*公開鍵(Public Key)*】ボックスにコピーし、逆方向のコピーも行います。さらに、それぞれのRSA鍵に対応するVPN IDタイプとVPN識別子を入力します。

- **ローカルX.509証明書(Local X.509 Certificate)**: 同様に、X.509証明書による認証方式も公開鍵と秘密鍵を使用します。X.509証明書には、公開鍵と、鍵の所有者を特定する情報が含まれています。このような証明書は、信頼される*認証局*(CA)によって署名され、発行されたものです。鍵交換中に証明書が交換され、ローカル保存されたCA証明書を使用して認証されます。リモートゲートウェイのX.509証明書がユニットにローカル保存されている場合、この認証タイプを使用してください。

- **リモートX.509証明書(Remote X.509 Certificate)**: リモートゲートウェイのX.509証明書がユニットにローカル保存されていない場合、この認証タイプを使用してください。リモートユニットで使用されている証明書のVPN IDタイプとVPN識

別子を選択する必要があります。この証明書は、*【サイト間VPN(Site-to-site VPN)】>>【IPsec】>>【詳細(Advanced)】*タブの*【ローカルX.509証明書(Local X.509 Certificate)】*エリアで選択されたものです。

VPN IDタイプ(VPN ID Type): 認証タイプによっては、VPN IDタイプとVPN識別子を選択する必要があります。ここで入力するVPN識別子は、リモートサイトで設定した値と一致している必要があります。サイト間VPNトンネルの確立に2台のASGアプライアンスを使用しているとします。ローカルユニットでの認証タイプとして*【RSA鍵(RSA Key)】*を選択する場合、VPN IDタイプとVPN識別子がリモートユニットの*【サイト間VPN(Site-to-site VPN)】>>【IPsec】>>【ローカルRSA鍵(Local RSA Key)】*タブでの設定と一致している必要があります。次のVPN IDタイプを選択できます。

- **IPアドレス**
- **ホスト名(Hostname)**
- **Eメールアドレス(E-mail Address)**
- **識別名(Distinguished Name)**: *リモートX.509証明書*認証のみで使用。
- **すべて(Any)**: *【応答のみ(Respond Only)】*ゲートウェイタイプのデフォルト。

リモートネットワーク(Remote Networks): リモートゲートウェイ経由でアクセス可能にするリモートネットワークを選択します。

コメント(Comment)(オプション): 説明などの情報を追加します。

3. **必要に応じて、詳細設定を行います。**
以下の詳細設定は、影響を理解している場合にのみ行ってください。

パスMTU検出をサポート(Support Path MTU Discovery): PMTU(パス最大伝送単位)とは、送信されるデータパケットのサイズです。IPデータパケットは、送信元から宛先までのパスのどこでもフラグメンテーション(断片化)を必要としない最大サイズにすることが望まれます。パス上の一部ルータにとって断片化しないで転送するには大き過ぎるデータパケットがある場合、そのルータはそれらを破棄して、*ICMP宛先不達*メッセージを「要断片化、DF設定」を意味するコードとともに返します。送信元ホストは、そのようなメッセージを受信すると、そのパスに対して想定されるPMTUを減らします。
このオプションを有効にすると、サーバ側でPMTUが有効になっている場合にASGがPMTUを有効化します。

輻輳シグナリングをサポート(Support Congestion Signaling)(ECN): ECN(明示的な輻輳通知)とはインターネットプロトコルの拡張であり、ネットワーク輻輳のエンドツー

エンドな通知をパケットのドロップなしで許可します。リモートエンドポイントおよび下位のネットワークと関与するルータがこれをサポートしている必要があります。

XAUTHクライアントモードの有効化(Enable XAUTH Client Mode): XAUTHとは、IPsec IKEの拡張であり、VPNゲートウェイでユーザ名とパスワードを使用してユーザを認証します。このリモートゲートウェイでの認証にXAUTHを使用するためには、このオプションを選択して、リモートゲートウェイの要求に従ってユーザ名とパスワード(2回)を入力します。

4. ***【保存(Save)】*****をクリックします。**
   ゲートウェイ定義が*【リモートゲートウェイ(Remote Gateways)】*リストに表示されます。

リモートゲートウェイ定義を編集または削除するには、対応するボタンをクリックします。

15.1.3ポリシ

*【IPsec】>>【ポリシ(Policies)】*タブでは、IPsecコネクション用のパラメータをカスタマイズし、ポリシに統合することができます。IPsecポリシは、IPsec接続のIKE(インターネット鍵交換)とIPsecプロポーザルパラメータを定義します。それぞれのIPsec接続にはIPsecポリシが必要です。

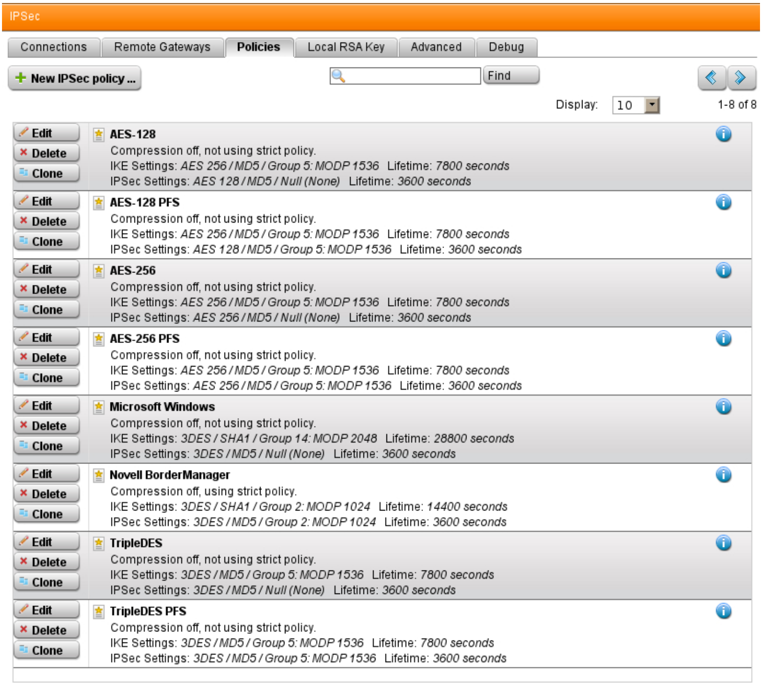


図132 サイト間VPN IPsec：ポリシリスト

IPsecポリシを作成するには、以下の手順に従います。

1. ***【ポリシ(Policy)】タブで、【新規IPsecポリシ(New IPsec Policy)】をクリックします。***
   *【IPsecポリシの追加(Add IPsec Policy)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name)：このポリシを説明する名前を入力します。

   IKE暗号化アルゴリズム(IKE Encryption Algorithm)：暗号化アルゴリズムでは、IKEメッセージの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

   - *DES*(56ビット)
   - *3DES*(168ビット)
   - *AES 128*(128ビット)
   - *AES 192*(192ビット)

- *AES 256*(256ビット)
- *Blowfish*(128ビット)
- *Twofish*(128ビット)
- *Serpent*(128ビット)

IKE認証アルゴリズム(IKE Authentication Algorithm): 認証アルゴリズムでは、IKEメッセージの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

- *MD5*(128ビット)
- *SHA1*(160ビット)
- *SHA2 256*(256ビット)
- *SHA2 384*(384ビット)
- *SHA2 512*(512ビット)

IKE SAライフタイム(IKE SA Lifetime): この値には、IKE SA(セキュリティアソシエーション)が有効な期間(つまり次の鍵更新を行うタイミング)を秒単位で指定します。有効な値は60秒～28800秒(8時間)です。デフォルト値は7800秒です。

IKE DHグループ(IKE DH Group): 接続をネゴシエートする際は、通信するパーティはデータの暗号化に使用する実際の鍵についても取り決めます。IKEはセッション鍵を生成するために、ランダムデータを利用する*Diffie-Hellman*(DH)アルゴリズムを使用します。ランダムデータの生成はプールビットに基づいて行われます。基本的にはIKEグループがプールビット数を知らせます。プールビット数が多いほど、ランダムな数字が大きくなります。数字が大きいほど、Diffie-Hellmanアルゴリズムの解読は難しくなります。結果として、プールビット数が多ければ安全ですが、CPUの使用量も増えます。現在は以下のDiffie-Hellmanグループがサポートされています。

- グループ1: MODP 768
- グループ2: MODP 1024
- グループ5: MODP 1536
- グループ14: MODP 2048
- グループ15: MODP 3072
- グループ16: MODP 4096

注 - グループ1(MODP 768)は弱く、相互運用性の理由からのみサポートされています。

IPsec暗号化アルゴリズム(IPsec Encryption Algorithm): IKEの場合と同じ暗号化アルゴリズム。

IPsec認証アルゴリズム(IPsec Authentication Algorithm): IKEの場合と同じ認証アルゴリズム。さらに、以下のアルゴリズムもあります。

SHA2 256(96ビット)

SHA2 384(96ビット)

SHA2 512(96ビット)

これらは、RFC 4868に準拠しないトンネルエンドポイント(V8以前のASGバージョンなど)への対応のために用意されています。そのため、96ビットより長い切り捨てられたチェックサムをサポートしません。

IPsec SAライフタイム(IPsec SA Lifetime): この値には、IPsec SAが有効な期間(つまり次の鍵更新を行うタイミング)を秒単位で指定します。有効な値は60秒～86400秒(1日)です。デフォルト値は7800秒です。

IPsec PFSグループ(IPsec PFS Group): *Perfect Forward Secrecy*(PFS)という概念では、セッション鍵を使用できなくなった場合に、この特定セッションのデータにのみアクセスを許可します。PFSが存在するには、IPsec SAの保護に使用される鍵は、IKE SAの鍵を取得するために使用されるランダム鍵作成用のマテリアルから派生したものではないことが必要です。その場合、PFSは2回目のDiffie-Hellman鍵交換を開始し、IPsec接続に対して選択されたDHグループが新たにランダム生成された鍵を取得することを提案します。サポートされているDiffie-HellmanグループはIKEの場合と同じです。
PFSを有効にすると安全性が高まりますが、交換にさらに時間がかかるようになります。低速なハードウェアではPFSは使用しないことをお勧めします。

注 - PFSはすべてのベンダーとの完全な相互運用性はありません。ネゴシエーション時に問題が発生したら、PFSを無効にしてください。

厳格なポリシ(Strict Policy): IPsecゲートウェイが暗号化アルゴリズムおよびその強度について提案を行うと、IPsecポリシがそれに対応していない場合でも、受信側ゲートウェイがこの提案を受け入れる場合があります。このオプションを選択すると、指定したパラメータを厳密にそのとおり使用することについてリモートエンドポイントが合意しないときは、IPsec

接続は確立されません。もし、ASG のIPsecポリシがAES-256暗号化を必要とする際に、SSH Sentinelを使用するロードウォリアがAES-128を使用して接続しようとすると、厳格なポリシオプションが有効である場合は、接続は拒否されます。

注 - 圧縮の設定は【*厳格なポリシ(Strict Policy)*】を介しては施行されません。

圧縮(Compression): このオプションでは、*IPペイロード圧縮プロトコル*(IPComp)によってIPパケットを暗号化の前に圧縮するかどうかを指定します。IPCompはIPパケットを圧縮してそのサイズを縮小し、通信ホストまたはゲートウェイのペア間の全体的な通信パフォーマンスを向上させます。デフォルトでは圧縮はオフになっています。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
新しいポリシが【*ポリシ(Policies)*】リストに表示されます。

ポリシを編集または削除するには、対応するボタンをクリックします。

15.1.4ローカルRSA鍵

RSA認証では、VPNエンドポイントの認証にRSA鍵が使用されます。エンドポイントの公開鍵は、接続が確立される前に手動で交換します。この認証タイプを使用する場合、VPN識別子を定義して、ローカルRSA鍵を作成する必要があります。ゲートウェイの公開RSA鍵を、Astaro Security Gatewayに対してIPsec RSA認証を使用するリモートIPsecデバイスで使用できるようにする必要があります。

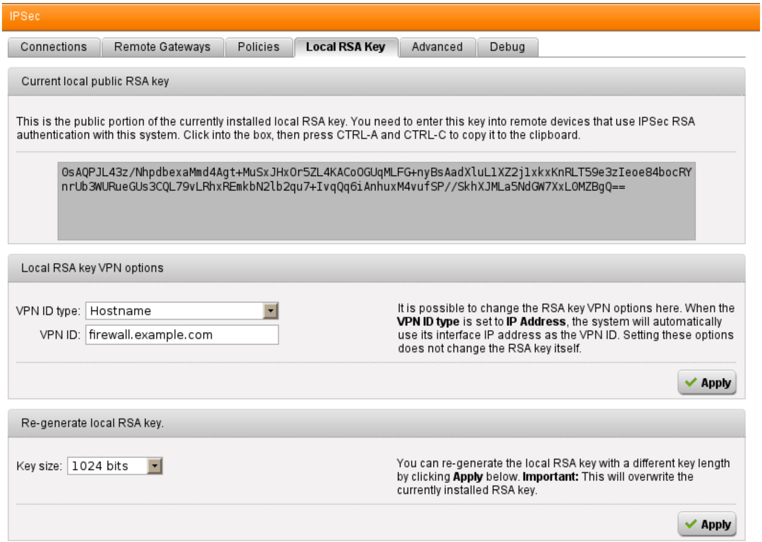


図133 サイト間VPN IPsec：ローカルRSA鍵の設定

現在のローカル公開RSA鍵(Current Local Public RSA Key)

現在インストールされているローカルRSA鍵ペアの公開部分が表示されます。ボックスをクリックし、`Ctrl-A`と`Ctrl-C`を押してクリップボードにコピーしてください。

ローカルRSA鍵VPNオプション(Local RSA Key VPN Options)

お客様のニーズに最適なVPN IDタイプを選択します。デフォルトでは、ゲートウェイのホスト名がVPN識別子として取得されます。スタティック(静的)IPアドレスをローカルVPNエンドポイントとする場合は、【*IPアドレス(IP Address)*】を選択します。あるいは、モバイルIPsecロードウォリアのVPN IDとしてEメールアドレスを使用することもできます。

- **ホスト名(Hostname)**：デフォルト設定はゲートウェイのホスト名です。ただし、ここで他のホスト名を入力することもできます。
- **Eメールアドレス(E-mail Address)**：デフォルトではゲートウェイのadminアカウントのEメールアドレスです。ただし、ここで他のEメールアドレスを入力することもできます。
- **IPアドレス(IP Address)**：ゲートウェイの外部インタフェースのIPアドレス。

設定を保存するには【*適用(Apply)*】をクリックします。設定を変更しても、RSA鍵に変化はありません。

ローカルRSA鍵の再生成(Re-generate Local RSA Key)

新しいRSA鍵を生成するには、希望する鍵サイズを選択し、*【適用(Apply)】*をクリックします。これにより、鍵生成プロセスが開始します。選択した鍵の長さと使用しているハードウェアに応じて、処理には数分から最大2時間かかる場合があります。鍵サイズ(鍵の長さ)は、1つの暗号で使用可能な鍵の数の尺度です。長さは通常、ビットで指定します。次の鍵サイズがサポートされています。

- 1024 ビット
- 2048 ビット
- 4096 ビット

RSA鍵を生成すると、適切な公開鍵が*【現在のローカル公開RSA鍵(Current Local Public RSA Key)】*ボックスに表示されます。新しいRSA鍵を生成すると、古い鍵が上書きされます。

15.1.5詳細

*【サイト間VPN(Site-to-site VPN)】>>【IPsec】>>【詳細(Advanced)】*タブで、IPsecVPNの詳細オプションを設定できます。希望の認証タイプに応じて、ローカル証明書(X.509認証の場合)やローカルRSA鍵(RSA認証の場合)などを定義可能です。この設定は熟練ユーザのみが行ってください。

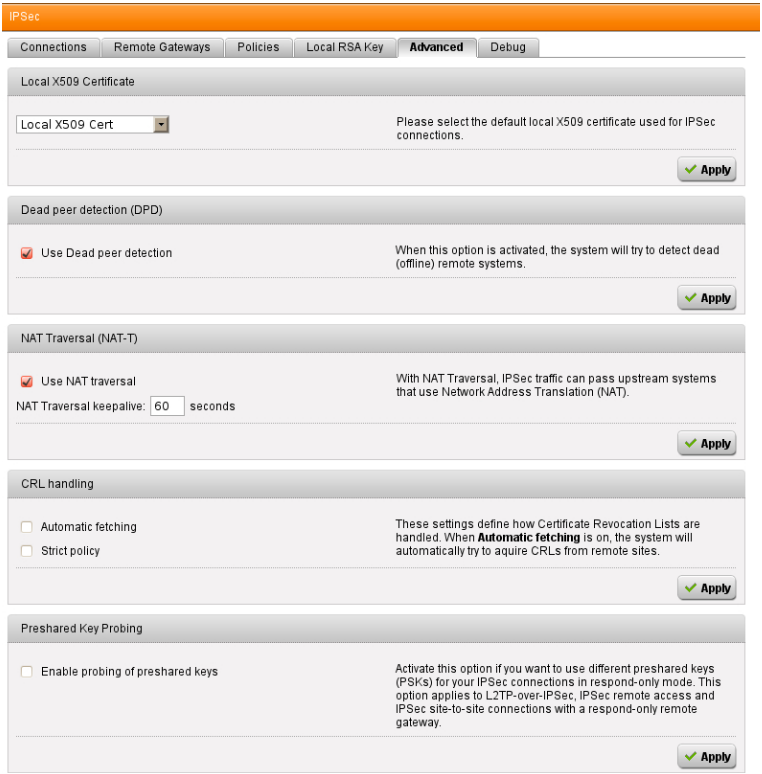


図134 サイト間VPN IPsec：詳細設定

ローカルX.509証明書

X.509認証では、証明書を使用してVPNエンドポイントの公開鍵を検証します この認証タイプを使用する場合は、*【ローカルX.509証明書(Local X.509 Certificate)】*エリアのドロップダウンリストからローカル証明書を選択する必要があります。選択した鍵/証明書は、X.509認証が選択された場合のリモートピアへのゲートウェイの認証に使用されます。

適切な秘密鍵がある証明書のみ選択できます。他の証明書はこのドロップダウンリストでは利用できません。

選択できる証明書がない場合、新しい証明書を作成するか、またはアップロード機能を使用してインポートして、*【証明書管理(Certificate Management)】*メニューで追加する必要があります。

証明書を選択したら、秘密鍵を保護するパスフレーズを入力します。パスフレーズは保存プロセスで確認され、パスフレーズが暗号化鍵と一致しない場合はエラーメッセージが表示されます。

アクティブな鍵/証明書を選択すると、それは【*ローカルX.509証明書(Local X.509 Certificate)*】エリアに表示されます。

デッドピア検出(DPD)

デッドピア検出を使用(Use Dead Peer Detection): デッドピア検出オプションを使用して、リモートVPNゲートウェイあるいはクライアントに接続できない場合は接続を自動的に終了します。スタティックエンドポイントとの接続では、トンネルは自動的に再ネゴシエートされます。ダイナミックエンドポイントとの接続では、リモート側でトンネルの再ネゴシエートを行うことが必要です。通常はこのオプションを常に有効にしておくほうが安全です。IPsecピアはリモート側がデッドピア検出をサポートするかどうかを自動的に判断し、必要に応じて通常モードにフォールバックします。

NAT-T(NATトラバーサル)

NATトラバーサルを使用(Use NAT Traversal): このオプションを選択すると、IPsecトラフィックは、*ネットワークアドレス変換*(NAT)を使用するアップストリームシステムを通過できるようになります。さらに、NATトラバーサルのキープアライブ(keepalive)間隔を定義できます。設定を保存するには【*適用(Apply)*】をクリックします。

CRLの取り扱い

証明書のプロバイダが、まだ有効な証明書に与えられる承認を取り消す場合があるかもしれません。たとえば、証明書の受取人が不正なデータ(名前など)を使ってそれを不正に取得したことが判明した場合や、証明書に埋め込まれた公開鍵の一部である秘密鍵を攻撃者が入手した場合は、証明書が失効します。そのような場合に備えて、いわゆる*証明書取り消しリスト*(CRL)が使用されます。CRLには通常、依然として有効期間は残っているものの無効とされた証明書のシリアル番号が含まれています。
これらの有効期限が切れると、証明書は無効になり、ブロックリストから削除されます。

自動フェッチ(Automatic Fetching): この機能は、HTTP、Anonymous(匿名)FTP、またはLDAPバージョン3を介しパートナー証明書で定義されたURLを通してCRLを要求します。有効期限が切れたら、要求によってCRLをダウンロードし、保存して更新できます。この機能を、ポート80または443を経由せずに使用する場合は、適切なファイアウォールルールを設定して、CRL配布サーバにアクセスできるようにしてください。

厳格なポリシ(Strict Policy): このオプションを有効にすると、対応するCRLのないパートナー証明書は拒否されます。

事前共有鍵プロービング

応答のみモードを使用したIPsec接続では、それぞれのIPsec接続に対して別々の事前共有鍵(PSK)を使用することを選択できます。

事前共有鍵のプロービングを有効にする(Enable probing of preshared keys): このチェックボックスにチェックを入れて、このオプションを有効にします。この設定は、L2TP-over-IPsec、リモートアクセスIPsec、VPN IPsecの各接続に影響を与えます。

15.1.6デバッグ

*【デバッグ(Debug)】*タブでIKE デバッグオプションを設定できます。どのタイプのIKEメッセージについてデバッグ出力を作成するかはチェックボックスで選択します。

注 –*【デバッグ(Debug)】*タブは、*【サイト間VPN IPsec(Site-to-site VPN IPsec)】*、*【リモートアクセスIPsec(Remote Access IPsec)】*、および*【Cisco VPN Client】*メニューで同じものが使用されています。

以下のフラグをログできます。

- **コントロール(Control)**: IKE ステートのコントロールメッセージを表示します。
- **発信(Emitting)**: 送信IKEメッセージのコンテンツを表示します。
- **構文解析(Parsing)**: 受信IKEメッセージのコンテンツを表示します。
- **Raw**: メッセージをrawバイトで表示します。
- **暗号化(Crypt)**: 暗号化および復号化のオペレーションを表示します。

15.2SSL

サイト間VPNトンネルはSSL接続を介して確立できます。SSL VPN接続には明確な役割があります。トンネルエンドポイントはクライアントまたはサーバとして機能します。常にクライアントが接続を開始し、サーバがクライアントの要求に応答します。これは、通常は両方のエンドポイントが接続を開始できるIPsecとは対照的です。

注 - 接続の確立に問題がある場合は、Webフィルタが透過モードで動作してSSLスキャンが有効になっているかどうかを確認してください。HTTPプロキシが透過モードで動作してSSLスキ

ャンが有効になっている場合は、VPN接続のターゲットホストが【*透過モードスキップリスト(Transparent Mode Skiplist)*】(【*Webセキュリティ(Web Security)*】>>【*Webフィルタリング(Web Filtering)*】>>【*詳細(Advanced)*】の下)に追加されていることを確認してください。

15.2.1接続

SSLVPNサイト間トンネルを作成するには、最初にサーバ設定を作成することが必要です。クライアントの設定は、常に2番目のステップで行います。

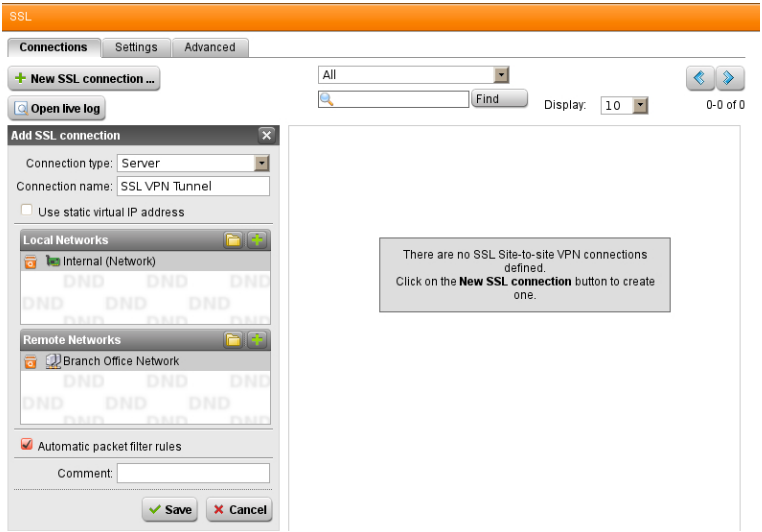


図135 サイト間SSL VPN:サーバ接続の設定

サーバ設定を作成するには、以下の手順に従います。

1. ***【コネクション(Connections)】タブで、【新規SSLコネクション(New SSL Connection)】をクリックします。***
   【SSL接続の追加(Add SSL Connection)】ダイアログボックスが開きます。

2. **次の設定を行います。**
   接続タイプ(Connection Type):ドロップダウンリストから【*サーバ(Server)*】を選択します。

   接続名(Connection Name):接続を説明する名前を入力します。

スタティック仮想IPアドレスを使用(オプション):このオプションは、IPアドレスプールがクライアントのネットワーク環境と互換でない場合のみ選択します。デフォルトでは、クライアントには*仮想IPプール(Vertual IP Pool)*(【*設定(Settings)*】タブで設定)からIPアドレスが割り当てられます。まれに、そのようなIPアドレスがクライアントホストですでに使用されている場合があります。そのような場合は、【*スタティックピアIP(Static Peer IP)*】フィールドに適切なIPアドレスを入力します。このIPアドレスは、トンネルセットアップ時にクライアントに割り当てられます。

ローカルネットワーク(Local Networks): リモートからのアクセスを許可する1つ以上のローカルネットワークを追加します。

リモートネットワーク(Remote Networks): ローカルネットワークへの接続を許可する1つ以上のリモートネットワークを追加します。

注 -【*ローカルネットワーク(Local Networks)*】と【*リモートネットワーク(Remote Networks)*】の設定は、後でクライアントの設定をやり直さずに変更できます。

自動ファイアウォールルール(Automatic Firewall Rules)(オプション):有効にすると、ASGは、アクセスするすべてのSSL VPNクライアントに対し、選択されたローカルネットワークへのアクセスを自動的に許可します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
   新しいSSLサーバ接続が【*接続(Connections)*】リストに表示されます。

4. **設定ファイルをダウンロードします。**
   新しく作成したSSLサーバ接続の行にある【*ダウンロード(Download)*】ボタンを使用して、この接続のクライアント設定ファイルをダウンロードします。

   設定ファイルの暗号化(Encrypt Configuration File)(オプション):セキュリティのために設定ファイルを暗号化することをお勧めします。パスワードを2回入力します。
   【*ピア設定のダウンロード(Download Peer Config)*】クリックしてファイルを保存します。
   このファイルは、クライアント側の管理者がトンネルのクライアントエンドポイントをセットアップする際に必要になります。

次のステップはクライアントの設定で、これはサーバ側ではなくクライアント側で行います。ダウンロードしたクライアント設定ファイルが手元にあることを確認してください。

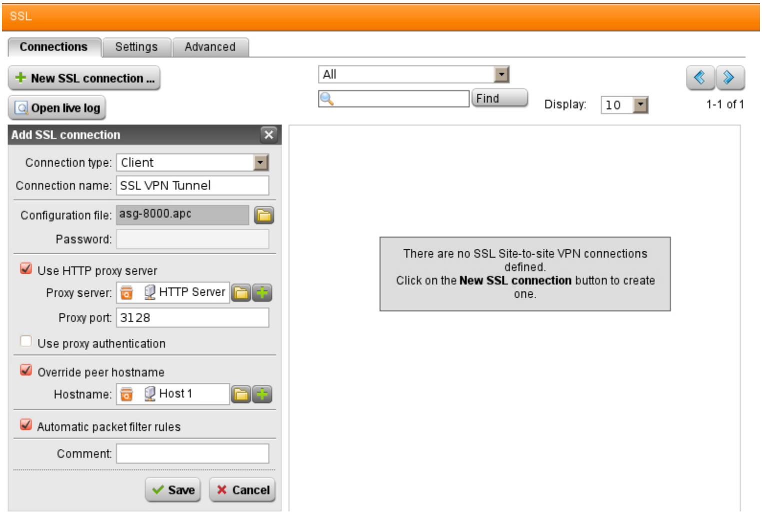


図136 サイト間SSL VPN:クライアント接続の設定

クライアント設定を作成するには、以下の手順に従います。

1. ***【コネクション(Connections)】タブで、【新規SSLコネクション(New SSL Connection)】をクリックします。***
   *【SSL接続の追加(Add SSL Connection)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   接続タイプ(Connection Type): ドロップダウンリストから*【クライアント(Client)】*を選択します。

   接続名(Connection Name): 接続を説明する名前を入力します。

   設定ファイル(Configuration File): フォルダアイコンをクリックし、クライアント設定ファイルを探して*【保存(Save)】*をクリックします。

   パスワード(Password)(オプション):ファイルが暗号化されている場合は、パスワードを入力します。

   HTTPプロキシサーバを使用(Use HTTP Proxy Server)(オプション):クライアントがプロキシの背後にある場合は、このチェックボックスにチェックを入れ、プロキシの設定を入力します。

プロキシ認証を使用(Use Proxy Authentication)(オプション):プロキシに対するクライアントの認証が必要な場合は、このチェックボックスにチェックを入れ、ユーザ名とパスワードを入力します。

ピアホスト名を無効にする(Override Peer Hostname)(オプション):サーバシステムの通常のホスト名(またはDynDNSホスト名)をクライアントホストで解決できない場合は、このチェックボックスにチェックを入れ、ホスト名をここに入力します。

自動ファイアウォールルール(Automatic Firewall Rules)(オプション):有効にすると、ASGは、トンネル化ローカルネットワークとトンネル化リモートネットワーク上のホスト間のトラフィックを自動的に許可します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   新しいSSL VPNクライアント接続が*【接続(Connections)】*リストに表示されます。

クライアント接続を編集または削除するには、対応するボタンをクリックします。

*【サイト間VPN(Site-to-site VPN)】*メニューをクリックすると、概要ページにSSL VPN接続のステータスが表示されます。接続が確立すると、ステータスアイコンが緑色に変わります。その後、トンネル両側の相互接続されたサブネットに関する情報も利用できるようになります。

15.2.2設定

【SSL】>>*【設定(Settings)】*タブで、SSL VPNサーバ接続の基本設定を設定できます。

> **注 –** このタブは*【サイト間VPN(Site-to-site VPN)】*>>*【SSL】*および*【リモートアクセス(Remote Access)】*>>*【SSL】*で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

図137 サイト間SSL VPN：設定

【サーバ設定(Server Settings)】

SSLVPN接続について以下の設定を行うことができます。

- **インタフェースアドレス(Interface Address)**：デフォルトは【*すべて(Any)*】です。Webアプリケーションファイアウォールを使用する場合、サービスがSSL接続をリスンするためのインタフェースアドレスを指定する必要があります。サイト間/リモートアクセスSSL接続ハンドラとWebアプリケーションファイアウォールが受信SSL接続を識別できるようにするために、この設定が必要です。

- **プロトコル(Protocol)**：使用するプロトコルを選択します。*TCP*または*UDP*を選択できます。

- **ポート(Port)**：ポートを変更できます。デフォルトのポートは443です。ポート10443、ACCゲートウェイマネージャポート4422、またはWebAdminインタフェースが使用しているポートは使用できません。

- **ホスト名を上書き(Override Hostname)**：【*ホスト名を上書き(Override Hostname)*】ボックスの値は、クライアントVPN接続のターゲットホスト名として使用され、デフォルトではゲートウェイのホスト名になります。システムの通常のホスト名(またはDynDNSホスト名)にこの名前でインターネットから到達できない場合のみ、デフォルトを変更します。

仮想IPプール(Virtual IP Pool)

プールネットワーク(Pool Network): これは、特定のIP範囲からSSLクライアントにIPアドレスを配布するために使用される仮想IPアドレスプールです。デフォルトでは、【*VPNプール(SSL)(VPN Pool (SSL))*】が選択されています。別のアドレスプールを選択する場合は、ネットマスクを29ビット以下にする必要があります。この理由は、OpenVPNはネットマスクが`/30`、`/31`、または`/32`のアドレスプールを扱えないからです。

CNをコピー(Duplicate CN)

ユーザが異なるIPアドレスから同時に接続できるようにする場合は、【*ユーザー毎の複数同時接続を許可(Allow Multiple Concurrent Connections Per User)*】を選択します。無効にすると、ユーザあたり1つの同時SSL VPN接続のみが可能になります。

15.2.3詳細

【*SSL*】>>【*詳細(Advanced)*】タブで、暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバオプションを設定できます。

> **注 –** このタブは【*サイト間VPN(Site-to-site VPN)*】>>【*SSL*】および【*リモートアクセス(Remote Access)*】>>【*SSL*】で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

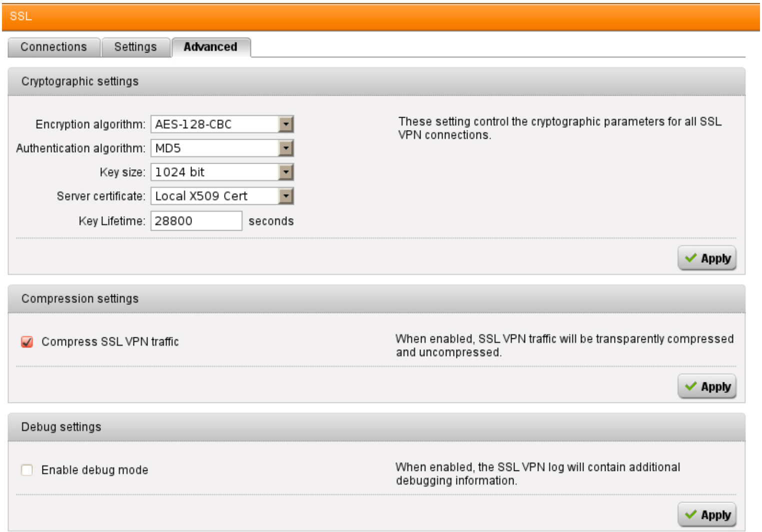


図138 サイト間SSL VPN: 詳細設定

【暗号設定(Cryptographic Settings)】

これらの設定で、すべてのSSLVPN リモートアクセスクライアントの暗号化パラメータを制御します。

- **暗号化アルゴリズム(Encryption Algorithm)**: 暗号化アルゴリズムは、VPNトンネルを通して送信されるデータの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。これらはすべて*暗号ブロック連鎖(Cipher Block Chaining)*(CBC)モードで動作します。
  - *DES-EDE3-CBC*
  - *AES-128-CBC*(128ビット)
  - *AES-192-CBC*(192ビット)
  - *AES-256-CBC*(256ビット)
  - *BF-CBC*(Blowfish(128ビット))
- **認証アルゴリズム(Authentication Algorithm)**: 認証アルゴリズムは、VPNトンネルを通して送信されるデータの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。
  - *MD5*(128ビット)
  - *SHA -1*(160ビット)

- **鍵サイズ(Key Size)**: 鍵サイズ(鍵の長さ)とは、Diffie-Hellman鍵交換の長さです。鍵が長ければ長いほど、対称鍵はセキュアになります。長さはビット単位で指定します。1024ビットまたは2048ビットの鍵サイズを選択できます。
- **サーバ証明書(Server Certificate)**: SSL VPNサーバがクライアントに対して自らの身元を証明するために使用するローカルSSL証明書を選択します。
- **鍵の有効期限**: 鍵の有効期限を入力します。デフォルトは28,800秒です。

圧縮設定(Compression Settings)

SSL VPNトラフィックを圧縮(Compress SSL VPN Traffic): 有効にすると、SSL VPNトンネルを通して送信されるすべてのデータは、暗号化の前に圧縮されます。

デバッグ設定(Debug Settings)

デバッグモードを有効化(Enable Debug Mode): デバッグモードを有効にすると、デバッグに役立つ多くの情報がSSL VPNログファイルに含まれます。

15.3証明書管理

*【サイト間VPN(Site-to-site VPN)】>>【証明書管理(Certificate Management)】*メニューは、Astaro Security Gatewayの認証関連のあらゆる操作を一元管理する場所です。たとえば、X.509証明書の作成またはインポートや、CRL*(証明書失効リスト)*のアップロードなどを行うことができます。

15.3.1証明書

*【サイト間VPN(Site-to-site VPN)】>>【証明書管理(Certificate Management)】>>【証明書(Certificates)】*タブで、X.509標準形式で公開鍵証明書を作成またはインポートできます。こうした証明書はデジタル署名された説明書で、通常は*認証局*(CA)が公開鍵およびX.500表記法による特定の*識別名*(DN)とともに発行します。

このタブで作成するすべての証明書は*認証局*(CA)によって自己署名されます。このCAは、WebAdminインタフェースへの初回ログイン時に提供した情報を使用して自動的に作成されたものです。

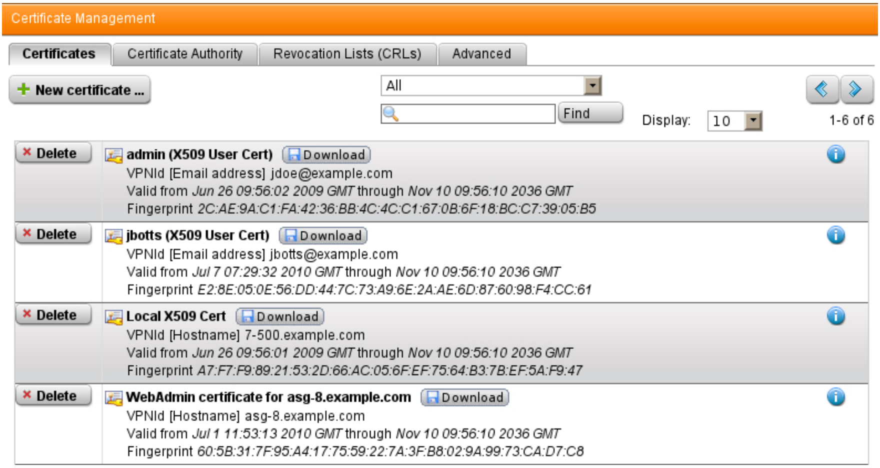


図139 証明書管理：証明書のリスト

証明書を生成するには、以下の手順に従います。

1. ***【証明書(Certificates)】タブで、【新規証明書(New Certificate)】をクリックします。***
   *【証明書の追加(Add Certificate)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name)：この証明書を説明する名前を入力します。

   方式(Method)：証明書を作成するには、*【生成(Generate)】*を選択します(証明書のアップロードに関する詳細は、以下を参照してください)。

   次の情報を指定します。

   - **VPN IDタイプ(VPN ID Type)**：証明書には一意の識別子を定義する必要があります。以下のタイプの識別子を使用できます。
     - Eメールアドレス(Email Address)
     - ホスト名(Hostname)
     - IP アドレス(IPアドレス)
     - 識別名(Distinguished Name)
   - **VPN ID**：選択したVPNID タイプに応じて、このテキストボックスに適切な値を入力します。たとえば、*【VPN IDタイプ(VPN ID Type)】*リストから*【IPアドレス(IP Address)】*を選択した場合、このテキストボックスにIPアドレスを入力します。*【VPN*

IDタイプ(VPN ID Type)】リストから【*識別名(Distinguished Name)*】を選択した場合は、このテキストボックスは非表示になります。

ドロップダウンリストおよび【*国(Country)*】から【*Eメール(Email)*】までのテキストボックスを使用して、証明書の所持者を特定する情報を入力します。この情報は【*識別名(Distinguished Name)*】を作成するために使用されます。つまり、その公開鍵を証明書が識別する団体の名前になります。この名前はX.500標準の多数の個人情報を含み、インターネット上で一意であると想定されます。証明書がロードウォリア接続用である場合は、【*一般名(Common Name)*】ボックスにユーザ名を入力します。証明書がホスト用である場合は、ホスト名を入力します。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
   証明書が【*証明書(Certificates)*】リストに表示されます。

証明書を削除するには、それぞれの証明書の【*削除(Delete)*】ボタンをクリックします。

または、証明書をアップロードするには、以下の手順に従います。

1. **【*証明書(Certificates)*】タブで、【*新規証明書(New Certificate)*】をクリックします。**
   【*証明書の追加(Add Certificate)*】ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name): この証明書を説明する名前を入力します。

   方式(Method):【*アップロード(Upload)*】を選択します。

   ファイルタイプ(File Type): 証明書のファイルタイプを選択します。以下のいずれかのタイプの証明書をアップロードできます。

   - **PKCS#12 コンテナ(PKCS#12 Container)**: PKCSは、RSAラボラトリにより考案され公開された公*開鍵暗号標準(Public Key Cryptography Standards)*(PKCS)のグループです。`PKCS#12`ファイル形式は一般的に、秘密鍵を公開鍵証明書とともにコンテナのパスフレーズで保護して保存するために使用されます。この形式のファイルをアップロードするには、このコンテナパスフレーズを知っていることが必要です(確認のためにパスフレーズを2回入力します)。
   - **PEMエンコード(PEM encoded)**: パスワード不要のBase64エンコードの*プライバシ強化メール*(`PEM`)ファイル形式。

   ファイル(File):【*ファイル(File)*】ボックスの隣りのフォルダアイコンをクリックし、アップロードする証明書を選択します。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
   証明書が【*証明書(Certificates)*】リストに表示されます。

証明書を削除するには、それぞれの証明書の【*削除(Delete)*】ボタンをクリックします。

証明書はPKCS#12またはPEM形式でダウンロードできます。PEMファイルは証明書だけを含みます。一方PKCS#12ファイルは、秘密鍵と署名に使用されたCA証明書を含んでいます。

注 -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (https://192.168.2.100など)を信頼されるサイトに追加します。これはIEの【*インターネットオプション*】>>【*セキュリティ*】で設定します。さらに、Internet Explorer 7を使用する場合は、【*信頼済みサイトゾーン*】で【*ファイルのダウンロード時に自動的にダイアログを表示*】を選択します。

15.3.2認証局

【*サイト間VPN(Site-to-site VPN)*】>>【*証明書管理(Certificate Management)*】>>【*認証局(Certificate Authority)*】タブで、ユニットに新しい*認証局*を追加できます。一般的に、*認証局*(CA)は、他のパーティが使用するデジタル証明書を発行する機関です。CAは、証明書に含まれる公開鍵が、その証明書に記載された人、組織、ホスト、あるいは他のエンティティに属することを、CA自身の証明書の秘密鍵を使って証明書の署名要求に署名することで証明します。このため、そのようなCAは署名CAと呼ばれます。

ASGでは、署名CAは、ASGへの最初のログイン時に提供した情報を使って自動的に作成されます。このように、【*証明書(Certificates)*】タブで作成するすべての証明書は、自己署名の証明書です。つまり、発行者と対象は同じになります。代わりに、サードパーティベンダの署名CAをインポートすることもできます。さらに、IPsec接続を要求するホストやユーザの真正性を確認する際に、秘密鍵が不明な別のCA証明書を使用することもできます。これらのCA証明書は確認CAと呼ばれ、このタブで追加できます。

重要 - お使いのシステムに複数の確認CAを持つことができますが、署名CAは1つだけしか持つことができません。新しい署名CAをアップロードすると、以前インストールされた署名CAは自動的に確認CAになります。

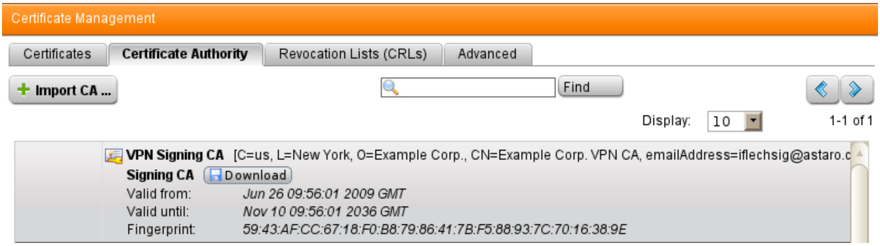


図140 証明書管理:認証局リスト

CAをインポートするには、以下の手順に従います。

1. ***【認証局(Certificate Authority)】タブで、【CAをインポート(Import CA)】をクリックします。***
   *【CAをインポート(Import CA)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): このCAを説明する名前を入力します。

   タイプ(Type): インポートするCAのタイプを選択します。確認CAと署名CAのいずれかを選択できます。確認CAはPEM形式で、署名CAはPKCS#12形式で利用できます。

   CA証明書(CA Certificate):*【CA証明書(CA Certificate)】*ボックスの隣りのフォルダアイコンをクリックして、インポートする証明書を選択します。新しい署名CAをアップロードする場合は、PKCS#12コンテナに使用されていたパスワードを入力する必要があります。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】をクリックします。***
   新しいCA証明書が*【認証局(Certificate Authority)】*リストに表示されます。

CAを削除するには、それぞれのCAの*【削除(Delete)】*ボタンをクリックします。

署名CAはPKCS#12形式でダウンロードできます。次にパスワードの入力を促すプロンプトが表示されます。このパスワードを使用してPKCS#12コンテナのセキュリティが保護されます。また、確認CAはPEM形式でダウンロードできます。

> **注** -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL(https://192.168.2.100など)を信頼されるサイトに追加します。これはIEの*【インターネットオプション】*>>*【セキュリティ】*で設定します。さらに、Internet Explorer 7を使用する場合は、*【信頼済みサイトゾーン】*で*【ファイルのダウンロード時に自動的にダイアログを表示】*を選択します。

15.3.3失効リスト

CRLは、失効したために使用できない証明書(正確にはシリアル番号)のリストです。*【サイト間VPN(Site-to-site VPN)】>>【証明書管理(Certificate Management)】>>【失効リスト(CRL)(Revocation Lists (CRLs))】*タブで、PKIで使用しているCRLをアップロードできます。

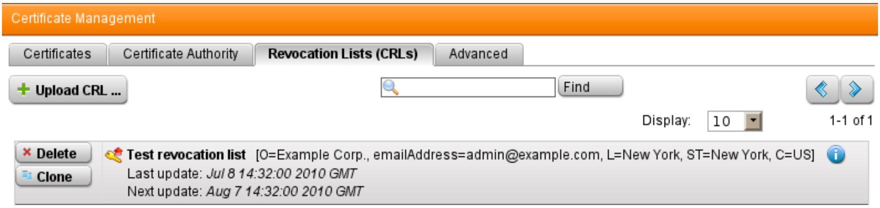


図141 証明書管理:失効リスト(CRL)の一覧

CRLをアップロードするには、以下の手順に従います。

1. ***【失効リスト(CRL)(Revocation Lists (CRLs))】タブで、【CRLをアップロード(Upload CRL)】をクリックします。***
   *【CRLをアップロード(Upload CRL)】*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name): このCRLを説明する名前を入力します。

   CRLファイル(CRL File):*【CRLファイル(CRL File)】*ボックスの隣りのフォルダアイコンをクリックし、アップロードするCRLを選択します。

   コメント(Comment)(オプション):説明などの情報を追加します。
3. ***【保存(Save)】をクリックします。***
   新しいCRLが失効リストの一覧に表示されます。

CRLを削除するには、それぞれのCRLの*【削除(Delete)】*ボタンをクリックします。

15.3.4詳細

*【サイト間VPN(Site-to-site VPN)】>>【証明書管理(Certificate Management)】>>【詳細(Advanced)】*タブで、ユニットの初期セットアップ時に作成されたVPN署名CAを再生成できます。VPN署名CAは、リモートアクセスやサイト間VPN接続に使用されるデジタル証明書に署名する認証局です。

署名CAの再生成(Re-generate Signing CA)

現在の署名CAを使用してすべてのユーザ証明書を更新できます。この機能は【*認証局(Certificate Authority)*】タブで別のVPN署名CAをインストールしたときに使用します。

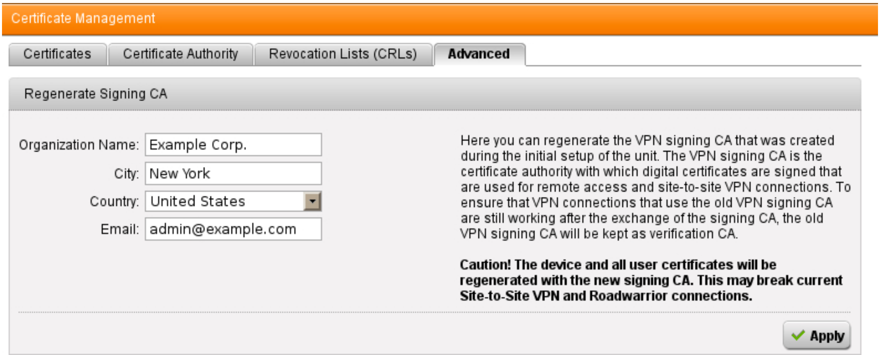


図142 証明書管理:詳細設定

１６リモートアクセス

この章では、当製品のリモートアクセス設定の構成方法について説明します。Astaro Security Gateway.Astaro Security Gatewayを使用したリモートアクセスは、*Virtual Private Network*(VPN)によって実現します。VPNは、テレコミューティング従業員などのリモートユーザに企業ネットワークへのアクセスを提供するためのセキュアでコスト効果の高い方法です。VPNはIPsec およびPPTP などの暗号化トンネリングプロトコルを使用して、VPNで伝送されるデータの機密性とプライバシを保護します。

クロスリファレンス - リモートアクセスVPN接続の設定方法の詳細は、Astaroナレッジベースを参照してください(「*ASG*「*バージョン7*」>>「*Astaroマニュアルおよびガイド*」の順にアクセスします)。

ASGは、それぞれのリモートアクセス接続タイプに必要なインストールおよび設定ファイルを自動的に生成します。これらのファイルはユーザポータルから直接ダウンロードできます。ただし、ユーザには、使用可能な接続タイプに対応するファイルのみが提供されます。たとえば、SSLリモートアクセスを使用できるユーザには、SSLインストールファイルのみが提供されます。

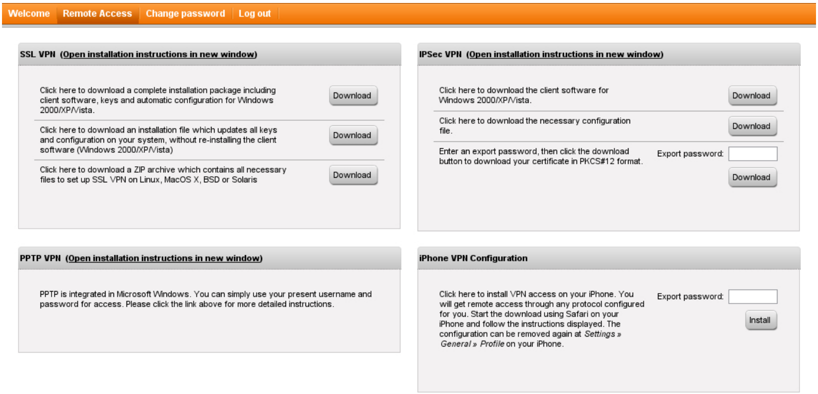


図143　ユーザポータル:リモートアクセスインストールファイル

【*リモートアクセスステータス(Remote Access Status)*】ページには、全オンラインユーザの概要が含まれます。

この章には次のトピックが含まれます。

- SSL
- PPTP
- L2TP over IPsec
- IPsec
- Cisco VPN Client
- 詳細
- 証明書管理

16.1SSL

Astaro Security GatewayのリモートアクセスSSL機能は、フル機能のSSLVPNソリューションであるOpenVPNによって実現します。これにより、お客様の会社とリモート従業員の間でポイントツーポイントの暗号化トンネルを作成することが可能になります。この機能では、インターネットリソースへのアクセスを許可するために、SSL証明書およびユーザ名/パスワードの組み合わせを必要とします。さらに、許可された各ユーザは、セキュアなユーザポータルから、カスタマイズされたSSL VPNクライアントソフトウェアバンドルをダウンロードできます。このバンドルには、無料のSSL VPNクライアント、SSL証明書、および簡単なワンクリックでインストールできる設定が含まれています。このSSL VPNクライアントは、ネイティブOutlook、ネイティブWindowsファイル共有などのほとんどのビジネスアプリケーションをサポートしています。

クロスリファレンス - SSL VPNクライアントの使用方法に関する詳細はAstaroナレッジベースを参照してください(*「ASG「バージョン7」>>「Astaroマニュアルおよびガイド」*の順にアクセスします)。

16.1.1グローバル

*【リモートアクセス(Remote Access)】>>【SSL】>>【グローバル(Global)】*タブで、VPNアクセスの基本的な設定を構成できます。デフォルトで、Astaro Security GatewayのSSLVPNソリューションは、スプリットトンネリングを採用しています。これは、リモートVPNユーザにVPN上のリソースへのアクセスを許可すると同時に、インターネットなどのパブリックネットワークへのアクセスを許可するプロセスです。ただし、以下の*【ローカルネットワーク(Local Networks)】*フィールドで*【すべて(Any)】*を選択すると、スプリットトンネリングをバイパスできます。その結果、すべてのトラフィックがVPN SSLトンネル経由でルーティングされます。この場合、ユーザにパブリックネットワークへのアクセスを許可するかどうかは、ファイアウォールの設定によって決まります。

図144 リモートアクセスSSL: SSLリモートアクセスの有効化

グローバルSSL VPNオプションを設定するには、以下の手順に従います。

1. ***【グローバル(Global)】タブで、SSLリモートアクセスを有効にします。***
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり、*【リモートアクセス設定(Remote Access Settings)】*エリアが編集可能になります。

2. **次の設定を行います。**
   ユーザとグループ(Users and Groups): SSL VPNリモートアクセスを使用できるようにするユーザとユーザグループを選択します。ユーザまたはユーザグループを指定しないと、SSLリモートアクセスを有効にできません。

   > **注** -ユーザポータルのSSL VPNクライアントソフトウェアバンドルは、*【ユーザとグループ(Users and Groups)】*ボックスで選択され、なおかつASGにユーザ定義があるユーザのみが使用できます(*「定義およびユーザおよびグループ」>>「ユーザ」*を参照)。ただし、これらのユーザも、ユーザポータルへはアクセスできます。

   ローカルネットワーク(Local Networks): SSLクライアントに到達可能にするローカルネットワークを選択します。

自動ファイアウォールルール(Auto Firewall Rules): 必要なファイアウォールルールを自動的に作成するには、このオプションを選択します。

3. ***【適用(Apply)】をクリックします。***
   設定が保存されます。

ライブログを開く(Open Live Log):

*【VPNライブログを開く(Open VPN Live Log)】*は、リモートアクセスアクティビティをログします。ボタンをクリックして、新しいウィンドウでライブログを開きます。

16.1.2設定

*【SSL】>>【設定(Settings)】*タブで、SSL VPNサーバ接続の基本設定を設定できます。

> **注 –** このタブは*【サイト間VPN(Site-to-site VPN)】>>【SSL】*および*【リモートアクセス(Remote Access)】>>【SSL】*で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

図145 リモートアクセスSSL:設定

【サーバ設定(Server Settings)】

SSLVPN接続について以下の設定を行うことができます。

- **インタフェースアドレス(Interface Address)**: デフォルトは【*すべて(Any)*】です。Webアプリケーションファイアウォールを使用する場合、サービスがSSL接続をリスンするためのインタフェースアドレスを指定する必要があります。サイト間/リモートアクセスSSL接続ハンドラとWebアプリケーションファイアウォールが受信SSL接続を識別できるようにするために、この設定が必要です。
- **プロトコル(Protocol)**: 使用するプロトコルを選択します。*TCP*または*UDP*を選択できます。
- **ポート(Port)**: ポートを変更できます。デフォルトのポートは`443`です。ポート`10443`、ACCゲートウェイマネージャポート`4422`、またはWebAdminインタフェースが使用しているポートは使用できません。
- **ホスト名を上書き(Override Hostname)**:【*ホスト名を上書き(Override Hostname)*】ボックスの値は、クライアントVPN接続のターゲットホスト名として使用され、デフォルトではゲートウェイのホスト名になります。システムの通常のホスト名(またはDynDNSホスト名)にこの名前でインターネットから到達できない場合のみ、デフォルトを変更します。

仮想IPプール(Virtual IP Pool)

プールネットワーク(Pool Network): これは、特定のIP範囲からSSLクライアントにIPアドレスを配布するために使用される仮想IPアドレスプールです。デフォルトでは、【*VPNプール(SSL)(VPN Pool (SSL))*】が選択されています。別のアドレスプールを選択する場合は、ネットマスクを29ビット以下にする必要があります。この理由は、OpenVPNはネットマスクが`/30`、`/31`、または`/32`のアドレスプールを扱えないからです。

CNをコピー(Duplicate CN)

ユーザが異なるIPアドレスから同時に接続できるようにする場合は、【*ユーザー毎の複数同時接続を許可(Allow Multiple Concurrent Connections Per User)*】を選択します。無効にすると、ユーザあたり1つの同時SSL VPN接続のみが可能になります。

16.1.3詳細

【*SSL*】>>【*詳細(Advanced)*】タブで、暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバオプションを設定できます。

注 – このタブは【サイト間VPN(Site-to-site VPN)】>>【SSL】および【リモートアクセス(Remote Access)】>>【SSL】で同じです。ここで加えた変更は、常に両方のSSL設定に影響を与えます。

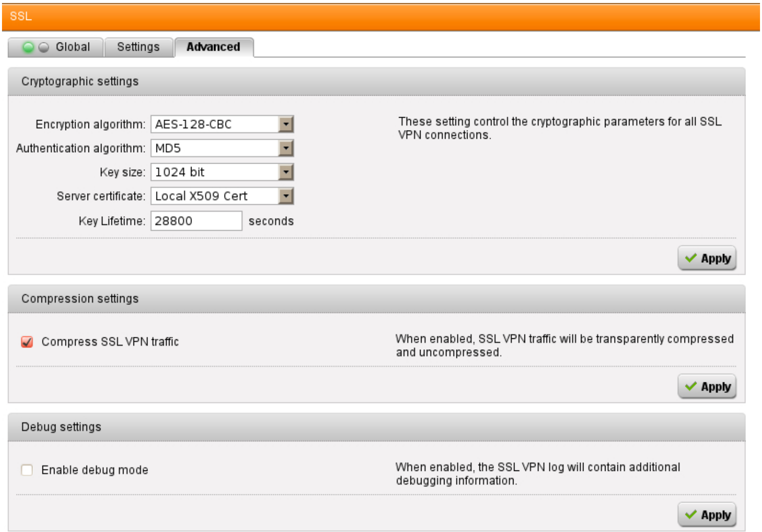


図146 リモートアクセスSSL:詳細設定

【暗号設定(Cryptographic Settings)】

これらの設定で、すべてのSSLVPN リモートアクセスクライアントの暗号化パラメータを制御します。

- **暗号化アルゴリズム(Encryption Algorithm)**: 暗号化アルゴリズムは、VPNトンネルを通して送信されるデータの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。これらはすべて*暗号ブロック連鎖(Cipher Block Chaining)*(CBC)モードで動作します。
  - *DES-EDE3-CBC*
  - *AES-128-CBC*(128ビット)
  - *AES-192-CBC*(192ビット)
  - *AES-256-CBC*(256ビット)
  - *BF-CBC*(Blowfish(128ビット))

- **認証アルゴリズム(Authentication Algorithm)**: 認証アルゴリズムは、VPNトンネルを通して送信されるデータの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。
  - *MD5*(128ビット)
  - *SHA -1*(160ビット)
- **鍵サイズ(Key Size)**: 鍵サイズ(鍵の長さ)とは、Diffie-Hellman鍵交換の長さです。鍵が長ければ長いほど、対称鍵はセキュアになります。長さはビット単位で指定します。1024ビットまたは2048ビットの鍵サイズを選択できます。
- **サーバ証明書(Server Certificate)**: SSL VPNサーバがクライアントに対して自らの身元を証明するために使用するローカルSSL証明書を選択します。
- **鍵の有効期限**: 鍵の有効期限を入力します。デフォルトは28,800秒です。

圧縮設定(Compression Settings)

SSL VPNトラフィックを圧縮(Compress SSL VPN Traffic): 有効にすると、SSL VPNトンネルを通して送信されるすべてのデータは、暗号化の前に圧縮されます。

デバッグ設定(Debug Settings)

デバッグモードを有効化(Enable Debug Mode): デバッグモードを有効にすると、デバッグに役立つ多くの情報がSSL VPNログファイルに含まれます。

16.2PPTP

PPTP(*Point-to-Point Tunneling Protocol*)により、単一のインターネットベースのホストは、暗号化トンネルを通して内部ネットワークサービスにアクセスすることが可能になります。PPTPの設定は容易で、Microsoft Windowsシステムでは特別なクライアントソフトウェアは必要ありません。

PPTPはWindows 95 以降のMicrosoft Windowsバージョンに含まれています。PPTPをAstaro Security Gatewayで使用するには、クライアントコンピュータがMSCHAPv2認証プロトコルをサポートすることが必要です。Windows 95および98のユーザがこのプロトコルをサポートするには、システムに更新パッケージを適用する必要があります。

16.2.1グローバル

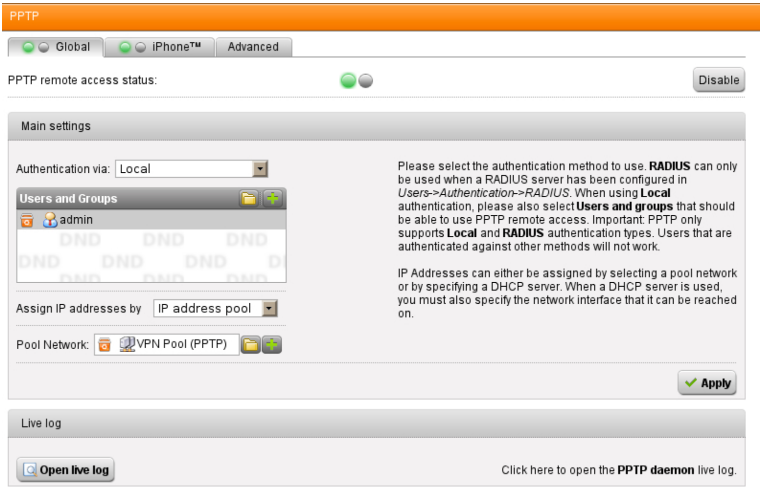


図147 PPTPリモートアクセス: PPTPリモートアクセスの有効化

グローバルPPTP オプションを設定するには、以下の手順に従います。

1. **【グローバル(Global)】タブで、PPTPリモートアクセスを有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり【*メイン設定(Main Settings)*】エリアが編集可能になります。

2. **次の設定を行います。**
   次を使用して認証(Authentication via): 認証メカニズムを選択します。PPTPリモートアクセスは、ローカルおよびRADIUS 認証のみをサポートしています。

   - **ローカル(Local)**:【*ローカル(Local)*】を選択した場合は、PPTPリモートアクセスを使用できるユーザやユーザグループを指定します。バックエンドのユーザグループをフィールドにドラッグすることはできません。ユーザアカウントを指定するまでは、PPTPリモートアクセスはアクティブにできません。

   > **注 -** SSL VPN同様、ユーザポータルの【*リモートアクセス(Remote Access)*】メニューにアクセスできるのは、【*ユーザとグループ(Users and Groups)*】ボックスで選

> 択されたユーザと、ユーザ定義がASGに定義されているユーザのみです。許可されたユーザがユーザポータルへのログインに成功すると、インストールに関する説明が表示されます。これはAstaroナレッジベースで提供されています(*【ASGバージョン7(ASG Version 7)】>>【リモートアクセス(Remote Access)】>>【PPTP】*の順に進みます)。

- **RADIUS**:*【RADIUS】*は、RADIUSサーバを事前に設定している場合にのみ選択できます。この認証方法では、ユーザは外部RADIUSサーバに対して認証されます。このサーバは*【定義およびユーザ(Definitions & Users)】>>【認証サーバ(Authentication】>>【サーバ(Servers)】*タブで設定できます。*【ユーザとグループ(Users and Groups)】*ダイアログボックスがグレーアウト表示されます。この設定はまだ変更できますが、影響はありません。RADIUSサーバはMSCHAPv2 チャレンジ/応答認証をサポートする必要があります。サーバはクライアントのIP アドレスやDNS/WINS サーバアドレスなどのパラメータを戻すことができます。PPTPモジュールは、NAS-IDとして「`pptp`」をRADIUSサーバに送信します。RADIUS認証を選択した場合は、ローカルユーザはPPTPでは認証できなくなることに注意してください。さらに、クライアントはMSCHAPv2認証もサポートする必要があることにも注意してください。

IPアドレスの割り当て方法(Assign IP Addresses By): IPアドレスは、事前に定義したIPアドレスプールから割り当てることも、DHCPサーバを使用して自動的に配布することもできます。

- **IPアドレスプール(IP Address Pool)**: PPTPによってリモートアクセスするクライアントに特定のIP範囲からIPアドレスを割り当てる場合は、このオプションを選択します。デフォルトでは、プライベートIPスペース`10.242.1.0/24`のアドレスが割り当てられます。このネットワーク定義は*VPNプール(PPTP)*と呼ばれ、すべてのネットワーク固有の設定オプションで使用できます。異なるネットワークを使用する場合は、*VPNプール(PPTP)*の定義を*【定義およびユーザ(Definitions & Users】>>【ネットワーク定義(Network Definitions)】*ページで変更します。または、*【プールネットワーク(Pool Network)】*テキストボックスの隣りの「+」アイコンをクリックして、別のIPアドレスプールを作成することもできます。

- **DHCPサーバ(DHCP Server)**:*【DHCPサーバ(DHCP Server)】*を選択する場合、DHCPサーバが接続に使用するネットワークインタフェースも指定する必要があります。DHCPサーバはインタフェースに直接接続する必要はありません。ルータを介してもアクセスできます。ローカルDHCPサーバはサポートされません。ここで選択したDHCPサーバは、物理的に異なるシステム上で稼働している必要があります。

3. ***【適用(Apply)】をクリックします。***
   設定が保存されます。

ライブログ

*PPTPデーモンライブログ*は、すべてのPPTPリモートアクセスアクティビティをログします。ボタンをクリックして、新しいウィンドウでライブログを開きます。

16.2.2iOSデバイス

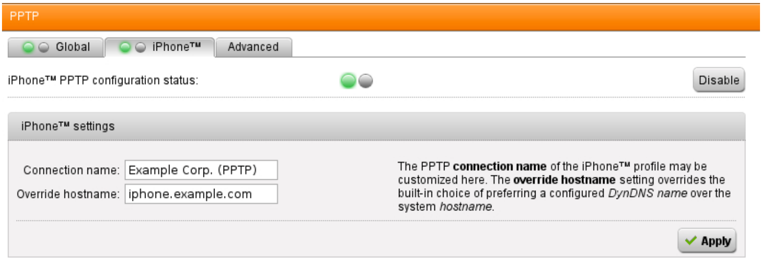


図148 PPTPリモートアクセス: iOSデバイス設定

ユーザポータルでiOSデバイスユーザに対しPPTPの自動設定を提供することができます。

ただし、*【グルーバル(Global)】*タブの*【ユーザとグループ(Users and Groups)】*ボックスに追加されたユーザのみが、ユーザポータルサイトで設定ファイルを表示できます。iOSデバイスのステータスはデフォルトで有効になっています。

接続名(Connection Name): PPTP接続を説明する名前を入力し、iOSデバイスのユーザがどの接続を確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後に次のプロトコルが続いたものになります: PPTP.

> **注 -** *【接続名(Connection Name)】*はすべてのiOSデバイス設定(PPTP、L2TP over IPsec、Cisco VPN Client)で一意である必要があります。

ホスト名を上書き(Override Hostname): システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって*【システムのDNSホスト名(System DNS Hostname)】*の前の*【DynDNSホスト名(DynDNS Hostname)】*の内部プリファレンスを上書きします。

iOSデバイスの自動設定を無効にするには、ステータスアイコンまたはタブのヘッダの*【無効(Disable)】*をクリックします。
ステータスアイコンが赤色に変わります。

16.2.3詳細

*【リモートアクセス(Remote Access)】>>【PPTP】>>【詳細(Advanced)】*タブで、暗号化の強度とPPTP リモートアクセスに関するデバッグ出力量を設定できます。PPTPの詳細オプションは、PPTPリモートアクセスのステータスが*【グローバル(Global)】*タブで有効になっていないと設定できません。

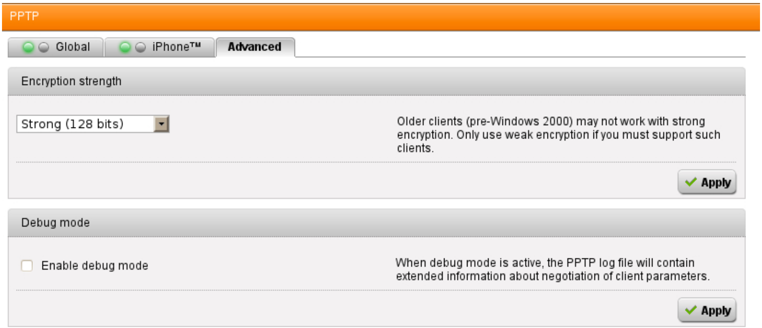


図149 PPTPリモートアクセス:詳細設定

暗号化の強度(Encryption Strength)

強い(128ビット)または弱い(40ビット)トンネル暗号化を選択できます(MPPE). 128ビット暗号化をサポートしないエンドポイントがない限り、弱い暗号化は使用しないでください。

デバッグモード(Debug Mode)

デバッグモードを有効化(Enable Debug Mode): このオプションで、PPTPログで生成されるデバッグ出力の量を制御します。接続で問題が発生し、クライアントパラメータのネゴシエーションに関する詳細な情報が必要である場合などに、このオプションを選択します。

16.3L2TP over IPsec

L2TP(*Layer Two(2)Tunneling Protocol*の略称)とは、既存のネットワーク(通常はインターネット)を介して2つのピア間でネットワークトラフィックをトンネリングするためのデータリンクレイヤ(OSIモデルのレイヤ2)プロトコルであり、VPNとも呼びます。L2TPプロトコルには機密性が欠けるため、多くの場合は機密性、認証、完全性を提供するIPsecと組み合わせて使用します。これら2つのプロトコルの組み合わせを別名「L2TP over IPsec」と呼びます。L2TP over IPsecを

使用すると、PPTPと同じ機能を提供しながら、暗号化されたIPsecトンネル経由のネットワークアクセスを個々のホストに提供することができます。

16.3.1 グローバル

*【L2TP over IPsec】>>【グローバル(Global)】*タブでは、L2TPover IPsec経由のリモートアクセスをセットアップするための基本オプションを設定できます。

図150 リモートアクセスL2TP: L2TPリモートアクセスを有効にする

L2TP over IPsecを使用するには、次の手順に従ってください。

1. ***【グローバル(Global)】*タブで、L2TP over IPsecを有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【サーバ設定およびIPアドレス割り当て(Server Settings and IP Address Assignment)】*エリアが編集可能になります。

2. **次の設定を行います。**
   インタフェース(Interface): L2TP VPNアクセスに使用するネットワークインタフェースを選択します。

   認証モード(Authentication Mode): 次の認証モードを選択できます。

- **事前共有鍵(Preshared Key)**: 事前共有鍵として使用されるパスワードを入力します。*事前共有鍵*方式では、通信を行う前に、通信当事者間で共有シークレットを交換します。通信のためには、シークレットを知っていることを両者が証明します。共有シークレットとは、L2TP用の暗号化アルゴリズムを使用してトラフィックを暗号化するために使用される安全なフレーズまたはパスワードです。セキュリティを高めるために、共有シークレットを強化する適切な手法をとる必要があります。共有シークレットのセキュリティは、パスワードの品質と、それをどれだけ安全に伝送するかにかかっています。一般的な言葉から成るパスワードは、辞書攻撃に対して非常に脆弱です。そのため、共有シークレットは非常に長くし、さまざまな文字、大文字、数字を組み合わせる必要があります。そのため、事前共有シークレットを使用する認証方式は、可能な限り証明書方式に切り替える必要があります。

  注 - iOSデバイスでは、PSK認証のみがサポートされているため、iOSデバイスへのアクセスを有効にするためには、*事前共有鍵*を選択する必要があります。

- **X.509 CAチェック(X.509 CA Check)**: X.509証明書により、参加者の多い大規模なVPNセットアップでの公開認証鍵の交換が容易になります。いわゆるCAがVPNエンドポイントの公開鍵を収集してチェックし、各メンバに対して証明書を発行します。証明書には、ピアのアイデンティティと公開鍵が含まれています。証明書はデジタル署名されているため、検出されずに他人が偽造証明書を発行することはできません。
  鍵交換中に証明書が交換され、ローカル保存されたCA公開鍵を使用して検証されます。続いて、公開鍵とプライベート鍵を使用してVPNエンドポイントの実際の認証が行われます。この認証モードを使用するためには、X.509証明書を選択します。
  X.509認証が機能するためには、*【リモートアクセス(Remote Access)】*>>*【認証管理(Certificate Management)】*>>*【認証局(Certificate Authority)】*タブで有効なCAを設定する必要があります。

IPアドレスの割り当て方法(Assign IP Addresses By): IPアドレスは、事前に定義したIPアドレスプールから割り当てることも、DHCPサーバを使用して自動的に配布することもできます。

- **プールネットワーク(Pool Network)**: デフォルトでは、IPアドレスの割当方法として*【IPアドレスプール(IP Address Pool)】*が選択されており、*【プールネットワーク(Pool Network)】*には事前定義済みの*【VPNプール(L2TP)(VPN Pool(L2TP))】*ネットワーク定義が選択されています。*VPNプール(L2TP)*とは、プライベートインターネット用のIPアドレススペース`10.x.x.x`からクラスCサブネットを使用してランダムに生成されたネットワークです。これは、ユーザが接続元として専用のア

ドレスプールを持つことを保証するものであり、通常は一切変更する必要がありません。別のネットワークを使用したい場合は、【*VPNプール(L2TP)(VPN Pool(L2TP))*】の定義を変更するか、ここでIPアドレスプールとして他のネットワークを割り当てます。

> **注 -** L2TP VPNプールに対してプライベートIPアドレスを使用しており、インターネットへのアクセスにIPsecホストを許可したい場合、適切なマスカレーディングまたはNATルールをIPアドレスプールに用意する必要があります。

- **DHCPサーバ(DHCP Server)**:【*DHCPサーバ(DHCP Server)*】を選択する場合、DHCPサーバが接続に使用するネットワークインタフェースも指定する必要があります。DHCPサーバはインタフェースに直接接続する必要はありません。ルータを介してもアクセスできます。ローカルDHCPサーバはサポートされません。ここで選択したDHCPサーバは、物理的に異なるシステム上で稼働している必要があります。

3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

   設定をキャンセルするには、【*有効化を中止(Abort Enable)*】またはアンバー色のステータスアイコンをクリックします。

アクセスコントロール(Access Control)

認証経路(Authentication Via): L2TPリモートアクセスは、ローカルおよびRADIUS 認証のみをサポートしています。

- **ローカル(Local)**:【*ローカル(Local)*】を選択する場合、L2TPリモートアクセスを使用できるようにするユーザとユーザグループを指定してください。バックエンドのユーザグループをフィールドにドラッグすることはできません。ローカルユーザの場合、通常の方法でユーザを追加し、これらのユーザに対してL2TPを有効にします。ユーザまたはグループを選択しない場合、L2TPリモートアクセスはオフになります。

> **注 -**SSLVPN同様、ユーザポータルの【*リモートアクセス(Remote Access)*】メニューにアクセスできるのは、【*ユーザとグループ(Users and Groups)*】ボックスで選択されたユーザと、ユーザ定義がASGに定義されているユーザのみです。認証モードに応じて、ユーザポータルへのログインに成功した認証ユーザには、IPsec事前共有鍵(認証モード「*事前共有鍵(Preshared key)*」)または`PKCS#12`ファイル(認証モード「*X.509 CAチェック(X.509 CA check)*」)ならびにインストール手順へのリンクがAstaroナレッジベースで

提供されます(*【ASGバージョン7(ASGVersion 7)】>>【リモートアクセス(Remote Access)】>>【L2TP over IPsec】*の順に選択)。

- **RADIUS**:*【RADIUS】*を選択すると、認証要求はRADIUSサーバに転送されます。L2TPモジュールは、NAS-IDとして「`l2tp`」をRADIUSサーバに送信します。

クライアントとサーバ間で、認証アルゴリズムのネゴシエーションが自動的に行われます。ローカルユーザに対し、Astaro Security Gatewayは次の認証プロトコルをサポートしています。

- MSCHAPv2
- PAP

デフォルトで、WindowsクライアントはMSCHAPv2をネゴシエーションします。

RADIUSユーザに対し、Astaro Security Gatewayは次の認証プロトコルをサポートしています。

- MSCHAPv2
- MSCHAP
- CHAP
- PAP

16.3.2iOSデバイス

ユーザポータルでiOSデバイスユーザに対し自動L2TP over IPsec設定を提供することができます。

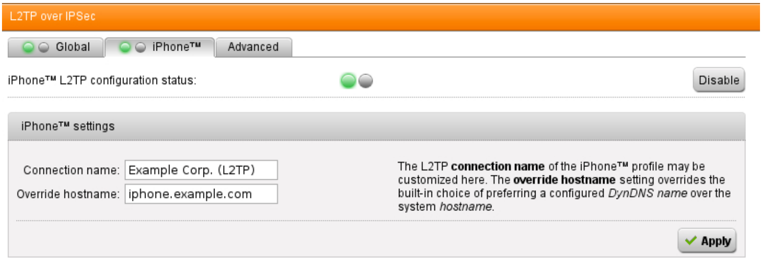


図151 リモートアクセスL2TP:iOSデバイス設定

ただし、*【グルーバル(Global)】*タブの*【ユーザとグループ(Users and Groups)】*ボックスに追加されたユーザのみが、ユーザポータルサイトで設定ファイルを表示できます。iOSデバイスのステータスはデフォルトで有効になっています。

接続名(Connection Name):L2TP over IPsec接続を説明する名前を入力し、iOSデバイスのユーザがどの接続を確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後に次のプロトコルが続いたものになります:L2TP over IPsec.

注 - *【接続名(Connection Name)】*はすべてのiOSデバイス設定(PPTP、L2TP over IPsec、Cisco VPN Client)で一意である必要があります。

ホスト名を上書き(Override Hostname): システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって*【システムのDNSホスト名(System DNS Hostname)】*の前の*【DynDNSホスト名(DynDNS Hostname)】*の内部プリファレンスを上書きします。

iOSデバイスの自動設定を無効にするには、ステータスアイコンまたはタブのヘッダの*【無効(Disable)】*をクリックします。
ステータスアイコンが赤色に変わります。

16.3.3詳細

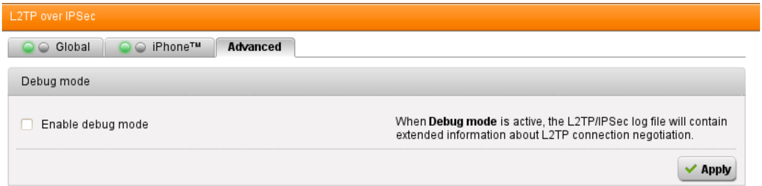


図152 リモートアクセスL2TP:詳細設定

デバッグモード(Debug Mode)

デバッグモードを有効化(Enable Debug Mode): このオプションは、L2TP over IPsecのログでどれくらいのデバッグ出力を生成するのかをコントロールします。接続で問題が発生し、クライアントパラメータのネゴシエーションに関する詳細な情報が必要である場合などに、このオプションを選択します。

16.4IPsec

IPsec(IP Security)とは、すべてのIPパケットを暗号化または認証すること(あるいはその両方)によってIP(*インターネットプロトコル*)通信のセキュリティを維持するための標準です。

IPsec標準は、次の2つのサービスモードと2つのプロトコルを定義しています。

- トランスポートモード
- トンネルモード
- *AH*(認証ヘッダ)認証プロトコル
- *ESP*(カプセル化セキュリティペイロード)暗号化(および認証)プロトコル

IPsecには、SA*(セキュリティアソシエーション)*と鍵配布を手動および自動で管理するための方法も用意されています。これらの特徴は、DOI*(解釈ドメイン)*で一元管理されています。

IPsecモード

IPsecは、トランスポートモードまたはトンネルモードで機能します。原則的に、ホスト間接続ではどちらのモードも使用できます。ただし、いずれかのエンドポイントがセキュリティゲートウェイである場合、トンネルモードを使用する必要があります。このASGでのIPsec VPN接続では、常にトンネルモードが使用されます。

トランスポートモードでは、元のIPパケットは他のパケットにカプセル化されません。元のIPヘッダは維持され、パケットの残りの部分は平文のまま(AH)またはカプセル化されて(ESP)送信されます。パケット全体をAHで認証することも、ESPでペイロードをカプセル化して認証することもできます。いずれの場合も、元のヘッダは平文としてWAN経由で送信されます。

トンネルモードでは、パケットヘッダとペイロードの全体が新しいIPパケットにカプセル化されます。IPヘッダがIPパケットに追加され、宛先アドレスは受信側トンネルエンドポイントに設定されます。カプセル化パケットのIPアドレスは変更なしで維持されます。続いて、元のパケットがAHで認証されるか、ESPでカプセル化されて認証されます。

IPsecプロトコル

IPsecでは、IP レベルで安全に通信するために2つのプロトコルを使用します。

- **AH(認証ヘッダ)**: パケット送信者を認証し、パケットデータの完全性を保証するためのプロトコル。
- **ESP(カプセル化セキュリティペイロード)**: パケット全体を暗号化し、そのコンテンツを認証するためのプロトコル。

AH(認証ヘッダ)プロトコルは、パケットデータの信頼性と完全性をチェックします。さらに、送信者と受信者のIPアドレスが送信中に変更されていないことをチェックします。パケットは、ハッシュベー

スのメッセージ認証コード(HMAC)と鍵を使用して作成されたチェックサムを使用して認証されます。次のいずれかのハッシュアルゴリズムが使用されます。

- **MD5(メッセージダイジェスト、バージョン5)**:このアルゴリズムでは、任意のサイズのメッセージから128ビットのチェックサムが生成されます。このチェックサムはメッセージの指紋のようなもので、メッセージが変更されるとチェックサムも変わります。このハッシュ値は、デジタル署名またはメッセージダイジェストとも呼ばれます。
- **SHA-1(セキュアハッシュ)**:このアルゴリズムではMD5と類似したハッシュが生成されますが、SHA-1ハッシュは長さが160ビットです。SHA-1は鍵がMD5より長いため、MD5より強力なセキュリティが実現します。

MD5と比較すると、SHA-1ハッシュは計算が難しく、生成に必要なCPU時間はより長くなります。もちろん、計算速度は、プロセッサの処理速度とAstaro Security Gatewayで使用されるIPsec VPN接続の数に依存します。

ESP(カプセル化セキュリティペイロード)プロトコルには、暗号化以外に、送信者を認証し、パケットコンテンツを検証する機能もあります。トンネルモードでESPを使用すると、IPパケット全体(ヘッダとペイロード)が暗号化されます。ここで、暗号化されていないIPヘッダとESPヘッダがカプセル化するパケットに追加されます。新しいIPヘッダには、受信側ゲートウェイと送信側ゲートウェイのアドレスが含まれています。これらのIPアドレスは、VPNトンネルのアドレスです。

暗号化付きのESPでは、通常次のアルゴリズムが使用されます。

- 3DES(トリプルデータ暗号化標準)
- AES(高度暗号化標準)

これらのうち、AESが最も安全です。AESで使用可能な鍵の有効長は128ビット、192ビット、256ビットです。Astaro Security Gateway は、多数の暗号化アルゴリズムをサポートしています。認証にはMD5またはSHA-1アルゴリズムを使用できます。

NAT-T(NATトラバーサル)

NAT トラバーサルとは、NATデバイスを使用するTCP/IPネットワーク内のホスト間で接続を確立するための技術です。この接続は、ESPパケットのUDPカプセル化を使用して、NATデバイス経由でIPsecトンネルを確立することによって実現します。UDPカプセル化は、IPsecピア間でNATが検出された場合のみに使用されます。検出されなかった場合は、通常のESPパケットが使用されます。

NATトラバーサルにより、ゲートウェイまたはロードウォリアをNATルータの背後に配置しながら、IPsecトンネルを確立できるようになります。この機能を使用する場合、両方のIPsecピア

でNATトラバーサルがサポートされている必要があります。ネゴシエーションは自動的に行われます。NATデバイスでIPseパススルーがオフになっていることを確認してください。オンになっていると、NATトラバーサルの使用に支障が出る可能性があります。

ロードウォリアでNATトラバーサルを使用したい場合、WebAdmin内の対応ユーザオブジェクトにスタティックリモートアクセスIPアドレス(RAS アドレス)が設定されている必要があります(WebAdminのユーザ定義 ページで【*スタティックリモートアクセスIPを使用(Use Static Remote Access IP)*】も参照してください)。

データ未送信時に確立されたトンネルが期限切れになることを防ぐために、NATトラバーサルのkeep-alive信号がデフォルトで60秒間隔で送信されます。keep-aliveメッセージは、NATルータがセッションに関連するステート情報を維持しており、トンネルが開いたままであることを確認するために送信されます。

TOS

「サービスタイプ」ビット(TOSビット)は、IPヘッダにあるいくつかの4ビットフラグです。これらのビットは、どのタイプのサービス品質が必要であるかを転送アプリケーションがネットワークに伝えることを許可するため、*サービススタイプビット*と呼ばれています。

Astaro Security GatewayへのIPsec導入では、TOSの値は常にコピーされます。

16.4.1 接続

【*IPsec*】>>【*コネクション(Connections)*】タブでは、IPsec接続を作成し、編集することができます。

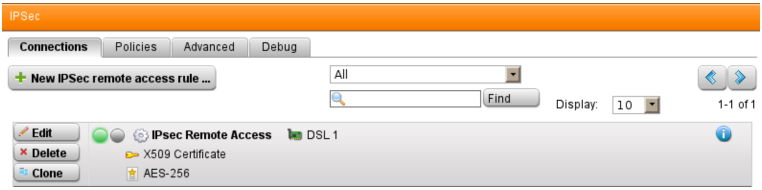


図153 リモートアクセスIPsec:接続リスト

IPsecコネクションを作成するには、次の手順に従います。

1. ***【コネクション(Connections)】タブで【新規IPsecリモートアクセスルール(New IPsec Remote Access Rule)】をクリックします。***

【*IPsecリモートアクセスルールの追加(Add IPsec Remote Access Rule)*】ダイアログボックスが開きます。

2. **次の設定を行います。**
名前(Name): このコネクションを説明する名前を入力してください。

インタフェース(Interface): IPsecトンネルのローカルエンドポイントとして使用されるインタフェースの名前を選択します。

ローカルネットワーク(Local Networks): VPNトンネル経由でアクセス可能にするローカルネットワークを選択します。

仮想IPプール(Virtual IP Pool): クライアントにスタティックIPアドレスが定義されていない場合、クライアントはこのIPアドレスプールに割り当てられたIPアドレスを取得します。デフォルトプールは*VPNプール(IPsec)*であり、プライベートIPスペース`10.242.4.0/24`から成ります。ただし、他のIPアドレスプールを選択または作成することもできます。

ポリシ(Policy): このIPsecコネクションのIPsecポリシを選択します。IPsecポリシは、【*リモートアクセス(Remote Access)*】>>【*IPsec*】>>【*ポリシ(Policies)*】タブで定義できます。

認証タイプ(Authentication Type): このリモートゲートウェイ定義の認証タイプを選択します。次のタイプを使用できます。

- **事前共有鍵(Preshared key)**: *事前共有鍵*(PSK)による認証では、秘密のパスワードを鍵として使用します。これらのパスワードは、接続を確立する前にエンドポイントに配布する必要があります。新しいVPNトンネルが確立されると、両端で、相手側が秘密のパスワードを知っていることのチェックが行われます。PSKのセキュリティは、使用するパスワードの品質に依存します。一般的な言葉や成句では、辞書攻撃に対して脆弱です。常時の、または長期的なIPsec接続では、パスワードの代わりに証明書を使用する必要があります。
- **X.509証明書(X.509 Certificate)**: X.509証明書による認証方式では、公開鍵と秘密鍵を使用します。X.509証明書には、公開鍵と、鍵の所有者を特定する情報が含まれています。このような証明書は、信頼される*認証局*(CA)によって署名され、発行されたものです。選択後、このIPsec接続の使用を許可するユーザを指定します。バックエンドユーザグループを【*許可されるユーザ(Allowed Users)*】フィールドにドラッグすることはできません。【*自動ファイアウォールルール(Automatic Firewall Rules)*】チェックボックスにチェックを入れた場合を除き、適切なファイアウォールルールを【*ネットワークセキュリティ(Network Security)*】メニューに手動で指定する必要があります。

> **注 -** ユーザポータルにアクセスできるのは、*【許可されるユーザ(Allowed Users)】*ボックスで選択されており、ASGにユーザ定義が存在するユーザのみです。ユーザポータルへのログインに成功した認証されたユーザには、AIC*(Astaro IPsec Client)*、設定ファイル、PKCS#12ファイル、インストール手順へのリンクがAstaroナレッジベースで提供されます(*【ASG Version 7】>>【リモートアクセス(Remote Access)】>>【IPsec】*の順に選択)。

- **CA DN照合(CA DN Match)**: この認証タイプでは、CA証明書のDN*(識別名)*の照合を使用して、VPNエンドポイントの鍵を検証します。選択した場合、*認証局*を1つ選択し、リモートアクセスクライアントのDNと一致する*DNマスク*を選択します。ここで、*【ピアサブネット範囲(Peer Subnet Range)】*を選択または追加します。クライアントは、いずれかの証明書がDNマスクと一致しなければ接続が許可されません。

XAUTHの有効化(Enable XAUTH)(オプション)設定されたバックエンドに対するユーザ認証が必要である場合は、拡張認証を有効にする必要があります。

自動ファイアウォールルール(Automatic Firewall Rules)(オプション):このオプションは、認証タイプ*X.509証明書*のみで使用可能です。
IPsec接続の確立に成功すると、各データトラフィックにファイアウォールルールが自動的に追加されます。接続が終了すると、パケットフィルタルールは削除されます。

コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**
新しいリモートアクセスルールが*【接続(Connections)】*リストに表示されます。

リモートアクセスルールを編集または削除するには、対応するボタンをクリックします。

16.4.2ポリシ

*【リモートアクセス(Remote Access)】>>【IPsec】>>【ポリシ(Policies)】*タブでは、IPsecコネクション用のパラメータをカスタマイズし、ポリシに統合することができます。IPsecポリシは、IPsec接続のIKE(インターネット鍵交換)とIPsecプロポーザルパラメータを定義します。それぞれのIPsec接続にはIPsecポリシが必要です。

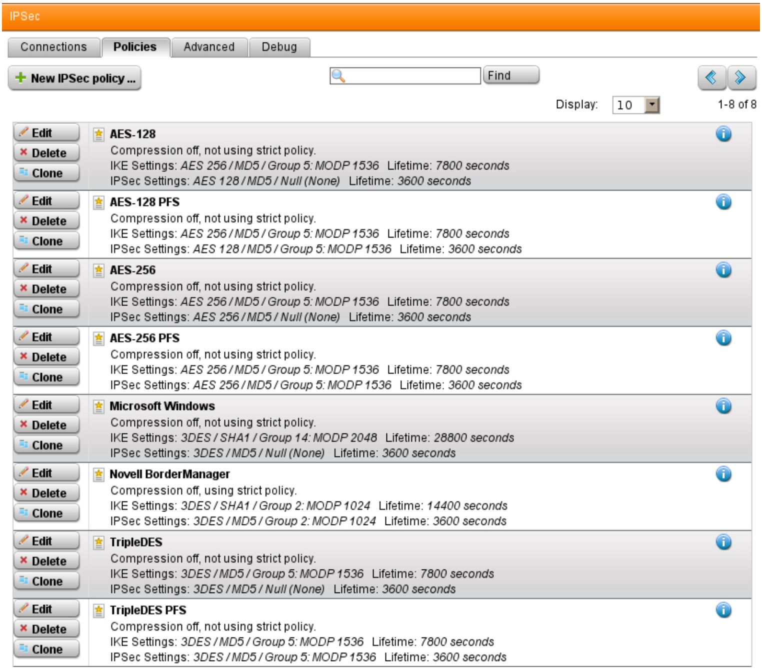


図154 リモートアクセスIPsec:ポリシリスト

IPsecポリシを作成するには、以下の手順に従います。

1. ***【ポリシ(Policy)】タブで、【新規IPsecポリシ(New IPsec Policy)】をクリックします。***
   *【IPsecポリシの追加(Add IPsec Policy)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name): このポリシを説明する名前を入力します。

   IKE暗号化アルゴリズム(IKE Encryption Algorithm): 暗号化アルゴリズムでは、IKEメッセージの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

   - *DES*(56ビット)
   - *3DES*(168ビット)
   - *AES 128*(128ビット)
   - *AES 192*(192ビット)
   - *AES 256*(256ビット)

- *Blowfish*（128ビット）
- *Twofish*（128ビット）
- *Serpent*（128ビット）

IKE認証アルゴリズム(IKE Authentication Algorithm)：認証アルゴリズムでは、IKEメッセージの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

- *MD5*（128ビット）
- *SHA1*（160ビット）
- *SHA2 256*（256ビット）
- *SHA2 384*（384ビット）
- *SHA2 512*（512ビット）

IKE SAライフタイム(IKE SA Lifetime)：この値には、IKE SA（セキュリティアソシエーション）が有効な期間（つまり次の鍵更新を行うタイミング）を秒単位で指定します。有効な値は60秒～28800秒（8時間）です。デフォルト値は7800秒です。

IKE DHグループ(IKE DH Group)：接続をネゴシエートする際は、通信するパーティはデータの暗号化に使用する実際の鍵についても取り決めます。IKEはセッション鍵を生成するために、ランダムデータを利用する*Diffie-Hellman*（DH）アルゴリズムを使用します。ランダムデータの生成はプールビットに基づいて行われます。基本的にはIKEグループがプールビット数を知らせます。プールビット数が多いほど、ランダムな数字が大きくなります。数字が大きいほど、Diffie-Hellmanアルゴリズムの解読は難しくなります。結果として、プールビット数が多ければ安全ですが、CPUの使用量も増えます。現在は以下のDiffie-Hellmanグループがサポートされています。

- グループ1：MODP 768
- グループ2：MODP 1024
- グループ5：MODP 1536
- グループ14：MODP 2048
- グループ15：MODP 3072
- グループ16：MODP 4096

注 - グループ1(MODP 768)は弱く、相互運用性の理由からのみサポートされています。

IPsec暗号化アルゴリズム(IPsec Encryption Algorithm): IKEの場合と同じ暗号化アルゴリズム。

IPsec認証アルゴリズム(IPsec Authentication Algorithm): IKEの場合と同じ認証アルゴリズム。さらに、以下のアルゴリズムもあります。

SHA2 256(96ビット)

SHA2 384(96ビット)

SHA2 512(96ビット)

これらは、RFC 4868に準拠しないトンネルエンドポイント(V8以前のASGバージョンなど)への対応のために用意されています。そのため、96ビットより長い切り捨てられたチェックサムをサポートしません。

IPsec SAライフタイム(IPsec SA Lifetime): この値には、IPsec SAが有効な期間(つまり次の鍵更新を行うタイミング)を秒単位で指定します。有効な値は60秒～86400秒(1日)です。デフォルト値は7800秒です。

IPsec PFSグループ(IPsec PFS Group):*Perfect Forward Secrecy*(PFS)という概念では、セッション鍵を使用できなくなった場合に、この特定セッションのデータにのみアクセスを許可します。PFSが存在するには、IPsec SAの保護に使用される鍵は、IKE SAの鍵を取得するために使用されるランダム鍵作成用のマテリアルから派生したものではないことが必要です。その場合、PFSは2回目のDiffie-Hellman鍵交換を開始し、IPsec接続に対して選択されたDHグループが新たにランダム生成された鍵を取得することを提案します。サポートされているDiffie-HellmanグループはIKEの場合と同じです。
PFSを有効にすると安全性が高まりますが、交換にさらに時間がかかるようになります。低速なハードウェアではPFSは使用しないことをお勧めします。

注 - PFSはすべてのベンダーとの完全な相互運用性はありません。ネゴシエーション時に問題が発生したら、PFSを無効にしてください。

厳格なポリシ(Strict Policy): IPsecゲートウェイが暗号化アルゴリズムおよびその強度について提案を行うと、IPsecポリシがそれに対応していない場合でも、受信側ゲートウェイがこの提案を受け入れる場合があります。このオプションを選択すると、指定したパラメータを厳密にそのとおり使用することについてリモートエンドポイントが合意しないときは、IPsec

接続は確立されません。もし、ASG のIPsecポリシがAES-256暗号化を必要とする際に、SSH Sentinelを使用するロードウォリアがAES-128を使用して接続しようとすると、厳格なポリシオプションが有効である場合は、接続は拒否されます。

注 - 圧縮の設定は【*厳格なポリシ(Strict Policy)*】を介しては施行されません。

圧縮(Compression): このオプションでは、*IPペイロード圧縮プロトコル*(IPComp)によってIPパケットを暗号化の前に圧縮するかどうかを指定します。IPCompはIPパケットを圧縮してそのサイズを縮小し、通信ホストまたはゲートウェイのペア間の全体的な通信パフォーマンスを向上させます。デフォルトでは圧縮はオフになっています。

コメント(Comment)(オプション):説明などの情報を追加します。

3. **【*保存(Save)*】をクリックします。**
新しいポリシが【*ポリシ(Policies)*】リストに表示されます。

ポリシを編集または削除するには、対応するボタンをクリックします。

16.4.3詳細

【*リモートアクセス(Remote Access)*】>>【*IPsec*】>>【*詳細(Advanced)*】タブで、IPsecVPNの詳細オプションを設定できます。希望の認証タイプに応じて、ローカル証明書(X.509認証の場合)やローカルRSA鍵(RSA認証の場合)などを定義可能です。この設定は熟練ユーザのみが行ってください。

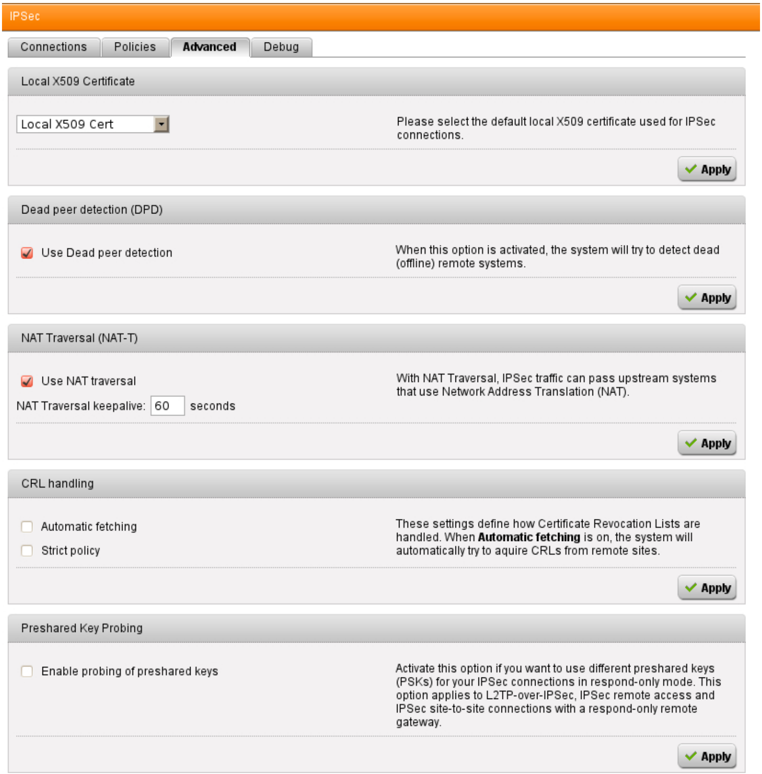


図155 リモートアクセスIPsec：詳細設定

ローカルX.509証明書

X.509認証では、証明書を使用してVPNエンドポイントの公開鍵を検証します この認証タイプを使用する場合は、【*ローカルX.509証明書(Local X.509 Certificate)*】エリアのドロップダウンリストからローカル証明書を選択する必要があります。選択した鍵/証明書は、X.509認証が選択された場合のリモートピアへのゲートウェイの認証に使用されます。

適切な秘密鍵がある証明書のみ選択できます。他の証明書はこのドロップダウンリストでは利用できません。

選択できる証明書がない場合、新しい証明書を作成するか、またはアップロード機能を使用してインポートして、【*証明書管理(Certificate Management)*】メニューで追加する必要があります。

証明書を選択したら、秘密鍵を保護するパスフレーズを入力します。パスフレーズは保存プロセスで確認され、パスフレーズが暗号化鍵と一致しない場合はエラーメッセージが表示されます。

アクティブな鍵/証明書を選択すると、それは【*ローカルX.509証明書(Local X.509 Certificate)*】エリアに表示されます。

デッドピア検出(DPD)

デッドピア検出を使用(Use Dead Peer Detection): デッドピア検出オプションを使用して、リモートVPNゲートウェイあるいはクライアントに接続できない場合は接続を自動的に終了します。スタティックエンドポイントとの接続では、トンネルは自動的に再ネゴシエートされます。ダイナミックエンドポイントとの接続では、リモート側でトンネルの再ネゴシエートを行うことが必要です。通常はこのオプションを常に有効にしておくほうが安全です。IPsecピアはリモート側がデッドピア検出をサポートするかどうかを自動的に判断し、必要に応じて通常モードにフォールバックします。

NAT-T(NATトラバーサル)

NATトラバーサルを使用(Use NAT Traversal): このオプションを選択すると、IPsecトラフィックは、*ネットワークアドレス変換*(NAT)を使用するアップストリームシステムを通過できるようになります。さらに、NATトラバーサルのキープアライブ(keepalive)間隔を定義できます。設定を保存するには【*適用(Apply)*】をクリックします。

CRLの取り扱い

証明書のプロバイダが、まだ有効な証明書に与えられる承認を取り消す場合があるかもしれません。たとえば、証明書の受取人が不正なデータ(名前など)を使ってそれを不正に取得したことが判明した場合や、証明書に埋め込まれた公開鍵の一部である秘密鍵を攻撃者が入手した場合は、証明書が失効します。そのような場合に備えて、いわゆる*証明書取り消しリスト*(CRL)が使用されます。CRLには通常、依然として有効期間は残っているものの無効とされた証明書のシリアル番号が含まれています。
これらの有効期限が切れると、証明書は無効になり、ブロックリストから削除されます。

自動フェッチ(Automatic Fetching): この機能は、HTTP、Anonymous(匿名)FTP、またはLDAPバージョン3を介しパートナー証明書で定義されたURLを通してCRLを要求します。有効期限が切れたら、要求によってCRLをダウンロードし、保存して更新できます。この機能を、ポート80または443を経由せずに使用する場合は、適切なファイアウォールルールを設定して、CRL配布サーバにアクセスできるようにしてください。

厳格なポリシ(Strict Policy): このオプションを有効にすると、対応するCRLのないパートナー証明書は拒否されます。

事前共有鍵プロービング

応答のみモードを使用したIPsec接続では、それぞれのIPsec接続に対して別々の事前共有鍵(PSK)を使用することを選択できます。

事前共有鍵のプロービングを有効にする(Enable probing of preshared keys): このチェックボックスにチェックを入れて、このオプションを有効にします。この設定は、L2TP-over-IPsec、リモートアクセスIPsec、VPN IPsecの各接続に影響を与えます。

16.4.4デバッグ

【*デバッグ(Debug)*】タブでIKE デバッグオプションを設定できます。どのタイプのIKEメッセージについてデバッグ出力を作成するかはチェックボックスで選択します。

> **注 –**【*デバッグ(Debug)*】タブは、【*サイト間VPN IPsec(Site-to-site VPN IPsec)*】、【*リモートアクセスIPsec(Remote Access IPsec)*】、および【*Cisco VPN Client*】メニューで同じものが使用されています。

以下のフラグをログできます。

- **コントロール(Control)**: IKE ステートのコントロールメッセージを表示します。
- **発信(Emitting)**: 送信IKEメッセージのコンテンツを表示します。
- **構文解析(Parsing)**: 受信IKEメッセージのコンテンツを表示します。
- **Raw**: メッセージをrawバイトで表示します。
- **暗号化(Crypt)**: 暗号化および復号化のオペレーションを表示します。

16.5Cisco VPN Client

Astaro Security Gateway は、Cisco VPNクライアント経由のIPsecリモートアクセスをサポートします。Cisco VPNクライアントは、Cisco Systemsの提供する実行可能プログラムです。これを使用すると、コンピュータのセキュリティを維持しながらVPN(*バーチャルプライベートネットワーク*)にリモート接続することができます。

16.5.1グローバル

*【リモートアクセス(Remote Access)】>>【Cisco VPNクライアント(Cisco VPN Client)】>>【グローバル(Global)】*タブでは、Cisco VPN クライアント経由のリモートアクセスをセットアップするための基本オプションを設定することができます。

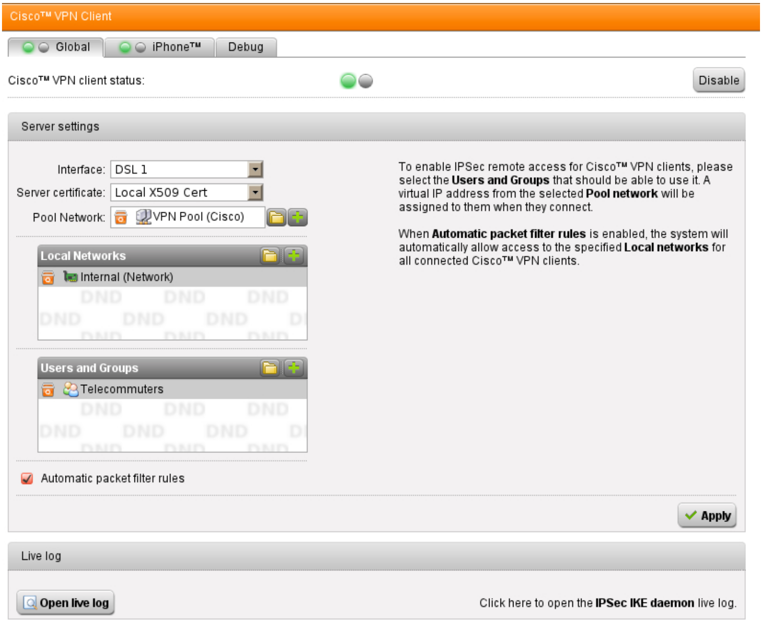


図156 Cisco VPNクライアント:Cisco VPNクライアント経由のリモートアクセスの有効化

Astaro Security Gatewayを設定してCisco VPNクライアント接続を許可するには、次の手順に従ってください。

1. ***【グローバル(Global)】*タブで、Cisco VPNクライアントを有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色になり、*【サーバ設定(Server Settings)】*エリアが編集可能になります。

2. **次の設定を行います。**
   インタフェース(Interface): Cisco VPNクライアント接続に使用するインタフェースを選択します。

サーバ証明書(Server Certificate): サーバがクライアントに対して自らの身元を証明するために使用する証明書を選択します。

プールネットワーク(Pool Network): 接続クライアントに仮想ネットワークアドレスを割り当てるために、仮想ネットワークアドレスを選択するためのネットワークプールを選択します。デフォルトで*【VPNプール(Cisco)(VPN Pool(Cisco))】*が選択されています。

ユーザとグループ(Users and Groups): Cisco VPNクライアント経由でASGに接続することが許可されるユーザまたはグループ(あるいはその両方)を選択します。ただし、バックエンドメンバシップグループをボックスにドラッグすることはできません。この理由は、IPsec設定時にユーザ証明書が必要であるにも関わらず、証明書はユーザが最初にログインに成功したときに初めて生成されるためです。

ローカルネットワーク(Local Networks): VPNトンネル経由でアクセス可能にするローカルネットワークを選択します。

自動ファイアウォールルール(Automatic Firewall Rules)(オプション): IPsec接続の確立に成功すると、各データトラフィックにファイアウォールルールが自動的に追加されます。接続が終了すると、パケットフィルタルールは削除されます。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

ライブログ

IPsec IKEデーモンログの接続ログを追跡するには、ライブログを使用します。ライブログには、接続の確立、維持、終了に関する情報が表示されます。

16.5.2iOSデバイス

ユーザポータルでiOSデバイスユーザに対しCisco IPsecの自動設定を提供することができます。

図157 Cisco VPNクライアント：iOSデバイス設定

ただし、*【グルーバル(Global)】*タブの*【ユーザとグループ(Users and Groups)】*ボックスに追加されたユーザのみが、ユーザポータルサイトで設定ファイルを表示できます。iOSデバイスのステータスはデフォルトで有効になっています。

接続名(Connection Name)：Cisco IPsec接続を説明する名前を入力し、iOSデバイスのユーザがどの接続を確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後に次のプロトコルが続いたものになります：CiscoIPsec.

> **注 -** *【接続名(Connection Name)】*はすべてのiOSデバイス設定(PPTP、L2TP over IPsec、Cisco VPN Client)で一意である必要があります。

ホスト名を上書き(Override Hostname)：システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって*【システムのDNSホスト名(System DNS Hostname)】*の前の*【DynDNSホスト名(DynDNS Hostname)】*の内部プリファレンスを上書きします。

iOSデバイスの自動設定を無効にするには、ステータスアイコンまたはタブのヘッダの*【無効(Disable)】*をクリックします。
ステータスアイコンが赤色に変わります。

VPN接続のオンデマンド確立(Establish VPN Connection On Demand)：ロケーションがホスト名またはいずれかのドメインと一致したときに接続を自動的に開始するには、このオプションを選択します。

接続するiOSデバイスに対し、*【グローバル(Global)】*タブに指定したサーバ証明書が提示されます。iOSデバイスは、この証明書のVPN IDがサーバのホスト名と一致しているかチェックし、異なる場合には接続を拒否します。サーバ証明書でVPN IDタイプに*【識別名(Distinguished*

Name)】を使用している場合、代わりに【*一般名(Common Name)*】フィールドが使用されます。サーバ証明書がこれらの制約を満たしていることを確認する必要があります。

16.5.3デバッグ

【*デバッグ(Debug)*】タブでIKE デバッグオプションを設定できます。どのタイプのIKEメッセージについてデバッグ出力を作成するかはチェックボックスで選択します。

> **注 –**【*デバッグ(Debug)*】タブは、【*サイト間VPN IPsec(Site-to-site VPN IPsec)*】、【*リモートアクセスIPsec(Remote Access IPsec)*】、および【*Cisco VPN Client*】メニューで同じものが使用されています。

以下のフラグをログできます。

- **コントロール(Control)**: IKE ステートのコントロールメッセージを表示します。
- **発信(Emitting)**: 送信IKEメッセージのコンテンツを表示します。
- **構文解析(Parsing)**: 受信IKEメッセージのコンテンツを表示します。
- **Raw**: メッセージをrawバイトで表示します。
- **暗号化(Crypt)**: 暗号化および復号化のオペレーションを表示します。

16.6詳細

【*リモートアクセス(Remote Access)*】>>【*詳細(Advanced)*】ページでは、リモートアクセスクライアントの詳細設定を行うことができます。ここで入力するDNSサーバとWINSサーバのIPアドレスは、ファイアウォールへの接続の確立時にリモートアクセスクライアントを使用するために提供され、これによってドメインの完全な名前解決を実現します。

図158 リモートアクセス(Remote Access):詳細設定

DNSサーバ(DNS Server): 組織のDNSサーバを最大2台指定します。

WINSサーバ(WINS Server): 組織のWINSサーバを最大2台指定します。WINS(*Windowsインターネットネーミングサービス*)とは、マイクロソフトがWindows OSに実装したNBNS(*NetBIOSネームサーバ*)です。DNSがドメイン名を対象にしているように、WINSはNetBIOS名を対象にしてホスト名とIPアドレスを一元的にマッピングします。

ドメイン名(Domain Name): 組織のFQDN(*完全修飾ドメイン名*)を入力します。完全修飾ドメイン名(FQDN)とは、DNSツリー階層でのノードの絶対位置を指定する明瞭なドメイン名です(`intranet.example.com`など)。

> **注** -PPTPおよびL2TP over IPsecの場合、ドメイン名は自動的に配信できず、クライアント側で設定する必要があります。

16.7認証管理

*【サイト間VPN(Site-to-site VPN)】>>【証明書管理(Certificate Management)】*メニューと*【リモートアクセス(Remote Access)】>>【証明書管理(Certificate Management)】*メニューには、同じ設定オプションが含まれています。これらの設定オプションを使用すると、Astaro Security Gatewayのすべての認証関連オプションを管理することができます。たとえば、X.509証明書の作成またはインポートや、CRL(*証明書失効リスト*)のアップロードなどを行うことができます。

16.7.1証明書

*「サイト間VPN」>>「証明書管理」>>「証明書」*を参照してください。

16.7.2認証局

「サイト間VPN」>>「証明書管理」>>「認証局」を参照してください。

16.7.3失効リスト

「サイト間VPN」>>「証明書管理」>>「失効リスト」を参照してください。

16.7.4詳細

「サイト間VPN」>>「証明書管理」>>「詳細」を参照してください。

17ログおよびレポーティング

この章では、Astaro Security Gatewayのログおよびレポーティング機能について説明します。

Astaro Security Gateway は、各種システムおよびネットワーク保護イベントを継続的に記録することにより、豊富なログ機能を提供します。詳細な監査証跡により、過去と現在のさまざまなネットワークアクティビティに関する分析が実現し、潜在的なセキュリティ上の脅威を特定したり、発生している問題のトラブルシューティングを行うことができます。

Astaro Security Gatewayのレポーティング機能は、現在のログデータを収集し、それをグラフ形式で表示することで、管理対象デバイスのリアルタイム情報を提供します。

WebAdminの【*ログパーティションステータス(Log Partition Status)*】ページは、ディスクの残容量、フィルアップレート(使用量増加速度)についての情報や、過去4週間のログパーティションの使用状況を示すヒストグラムなど、Astaro Security Gatewayユニットのログパーティションのステータスを示します。フィルアップレートは、測定地点と開始地点の差分を経過時間で割って計算するため、当初は値がやや不正確になりますが、システムの稼働時間が長くなればなるほど精度が増します。

この章には次のトピックが含まれます。

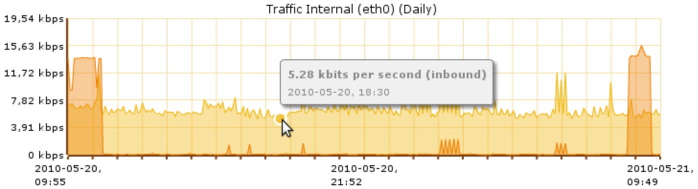
- ログファイルの閲覧
- ハードウェア
- ネットワーク使用状況
- ネットワークセキュリティ
- Webセキュリティ
- メールセキュリティ
- リモートアクセス
- Webアプリケーションファイアウォール
- エグゼクティブレポート
- ログ設定
- レポーティング設定

Flashベースのレポーティング

バージョン8から、Astaro Security Gateway レポートのデータグラフは、デフォルトで、Adobe® Flash®アニメーションとして表示されます。これらのFlashグラフにより、これまで使用されてきた静止画像より、グラフの構成情報にきめ細かくアクセスすることが可能となっています。ただし、V7のレポート形式のほうが望ましい場合は、プリファレンスを変更して静止画像に戻すことができます(「マネジメント」>>「*WebAdmin設定*」>>「*ユーザ設定*」を参照)。

折れ線グラフ

Flash折れ線グラフと簡単にインタラクティブ操作できます。マウスのカーソルをグラフ上に置くと、大きなドット(点)が表示され、グラフのその部分の詳細な情報が表示されます。このドットは、グラフの線に沿って移動します。マウスのカーソルを移動すると、ドットもそれに従って移動します。グラフに何本かの線がある場合、ドットはマウスカーソルの移動に従って線の間を移動します。さらに、ドットの色は、それが表示している情報がどの線に関連するかによって変わるため、線が互いに近接している場合に役立ちます。



	Maximum	Minimum	Average	Last
Interface Usage Internal (eth0) (inbound)	12.62 kbps	5.08 kbps	6.59 kbps	5.98 kbps
Interface Usage Internal (eth0) (outbound)	16.01 kbps	0.00 bps	1.47 kbps	70.00 bps

図159 レポーティング: Flashベースの折れ線グラフの例

円グラフ

Flash折れ線グラフと同様に、円グラフとも対話可能:マウスのカーソルを円グラフの一部に置きます。すると、その部分は円グラフの他の部分から即座に切り離され、その部分の詳細な情報がツールヒントに表示されます。

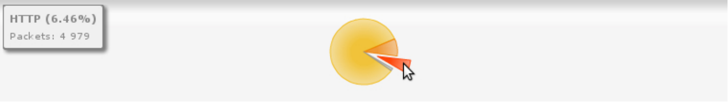


図160 レポーティング: Flashベースの円グラフの例

17.1 ログファイルの閲覧

*【ログおよびレポーティング(Logging & Reporting)】>>【ログファイルの閲覧(View Log Files)】*メニューで、各種ログファイルを表示および検索できます。

17.1.1 今日のログファイル

*【ログおよびレポーティング(Logging & Reporting)】>>【ログファイルの閲覧(View Log Files)】>>【今日のログファイル(Today's Log Files)】*タブで、現在のすべてのログに容易にアクセスできます。

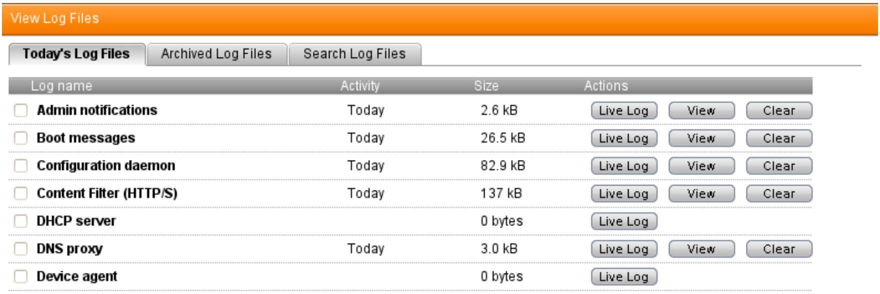


図161 ログ: 今日のログファイル

このタブでは、すべてのログファイルに適用できるさまざまな作業を実行できます。次の作業を実行できます。

- **ライブログを開く(Open Live Log):**ポップアップウインドウが開き、リアルタイムでログファイルを表示できます。新しいアクティビティが発生すると、リアルタイムでログファイルに新しい行が追加されます。*【自動スクロール(Autoscroll)】*を選択すると、ポップアップウインドウが自動的にスクロールダウンして、常に最新のログが表示されます。さらに、ポップアップウインドウにはフィルタテキストボックスも含まれており、これによって新しいログの表示ををフィルタに一致するレコードだけに制限できます。
- **表示(View)**: ポップアップウィンドウが開き、ログファイルが現在の状態で表示されます。
- **クリア(Clear)**: ログファイルのコンテンツを削除します。

テーブル下部のドロップダウンリストを使用して、選択したログファイルをzipファイル形式でダウンロードしたり、それらのコンテンツを同時に削除したりできます。

注 -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL(https://192.168.2.100など)を信頼されるサイトに追加します。これはIEの*【インターネットオプション】*>>*【セキュリティ】*で設定します。さらに、Internet Explorer 7を使用する場合は、*【信頼済みサイトゾーン】*で*【ファイルのダウンロード時に自動的にダイアログを表示】*を選択します。【ライブログ(Live Log)】ポップアップでは、行の追加が停止する場合があります。このような問題が発生した場合は、【ライブログ(Live Log)】ウインドウ内でF5(再表示)を押してください。

17.1.2アーカイブログファイル

*【ログ(Logging)】&【レポーティング(Reporting)】>>【ログファイルの閲覧(View Log Files)】>>【アーカイブログファイル(Archived Log Files)】*タブで、ログファイルアーカイブを管理することができます。すべてのログファイルはデイリーベースでアーカイブされます。アーカイブしたログファイルにアクセスするには、ログが書き込まれているAstaro Security Gatewayのサブシステムと年月を選択します。

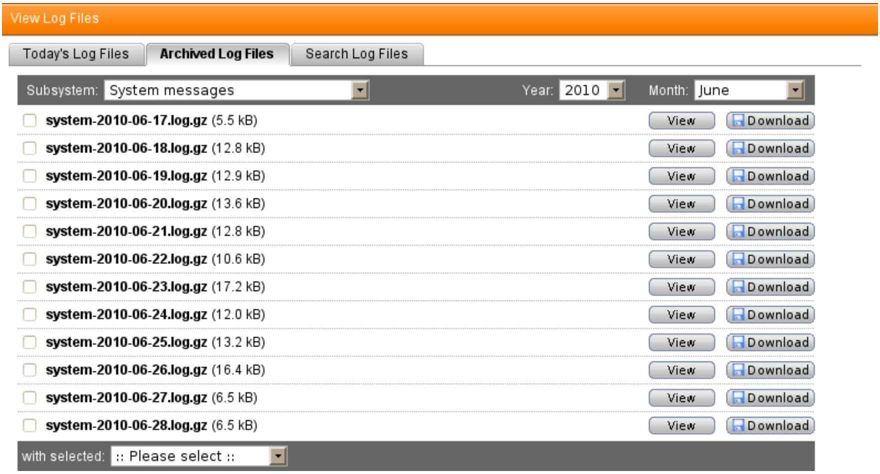


図162 ログ:アーカイブログファイル

選択に一致したすべての利用できるログファイルが年代順に表示されます。アーカイブしたログファイルは、閲覧したり、zipファイル形式でダウンロードできます。

テーブル下部のドロップダウンリストを使用して、選択したログファイルを`zip`ファイル形式でダウンロードしたり同時に削除したりすることができます。

> **注** -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL(`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの【*インターネットオプション*】>>【*セキュリティ*】で設定します。さらに、Internet Explorer 7を使用する場合は、【*信頼済みサイトゾーン*】で【*ファイルのダウンロード時に自動的にダイアログを表示*】を選択します。

17.1.3ログファイルの検索

【*ログおよびレポーティング(Logging & Reporting)*】>>【*ログファイルの閲覧(View Log Files)*】>>【*ログファイルの検索(Search Log Files)*】タブで、さまざまな期間のローカルログファイルを検索できます。最初に、検索するログファイルを選択し、次に検索する語句を入力して、検索期間を選択します。【*期間の選択(Select Time Frame)*】リストから【*カスタム期間(Custom Time Frame)*】を選択した場合は、開始日と終了日を指定できます。【*検索開始(Start Search)*】ボタンをクリックすると、ポップアップウインドウにクエリ結果が表示されます。ブラウザによっては、WebAdmin用にポップアップウインドウを許可する必要があります。

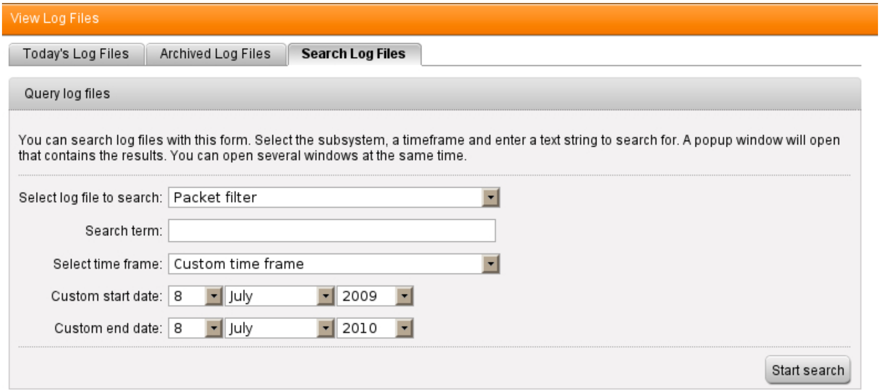


図163 ログ:ログファイルの検索

17.2ハードウェア

【*ログおよびレポーティング(Logging & Reporting)*】>>【*ハードウェア(Hardware)*】メニューには、さまざまな期間におけるハードウェアコンポーネントの使用状況に関する概要的な統計が表

示されます。

17.2.1デイリー

*【ハードウェア(Hardware)】>>【デイリー(Daily)】*タブは、次のハードウェアコンポーネントに関する過去24時間の統計概観を示します。

- CPU の使用状況
- メモリ/スワップの使用状況
- パーティションの使用状況

CPUの使用状況(CPU Usage): ヒストグラムに、現在のプロセッサ使用状況(%)が表示されます。

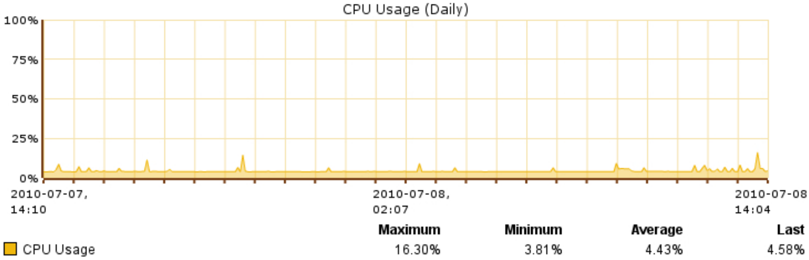


図164 レポーティング(Reporting):CPU使用状況のヒストグラム

メモリ/スワップの使用状況(Memory/Swap Usage): メモリとスワップの使用状況(%)。スワップの使用状況は、システム構成によって大きく異なります。侵入防御やプロキシサーバなどのサービスをアクティブにすると、メモリの使用率が高くなります。システムのメモリが不足すると、スワップスペースが使用されるようになり、システム全体のパフォーマンスが低下します。スワップスペースの使用はできるだけ低く抑える必要があります。このためには、システムで利用できるメモリの合計容量を増やします。

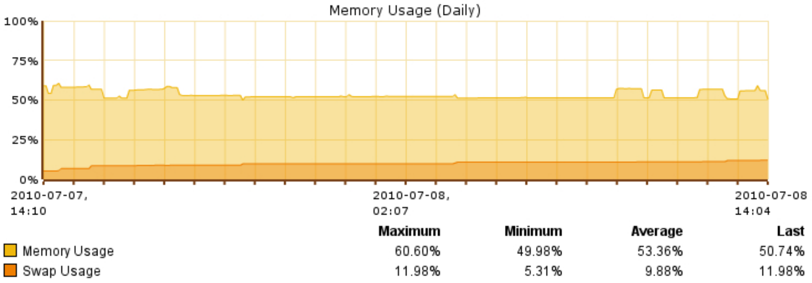


図165 レポーティング(Reporting):メモリ/スワップ使用状況のヒストグラム

パーティション使用状況(Partition Usage): 選択されたパーティションの使用状況(%)。すべてのチャートには3つのグラフが表示され、それぞれが1つのハードディスクドライブパーティションを示します。

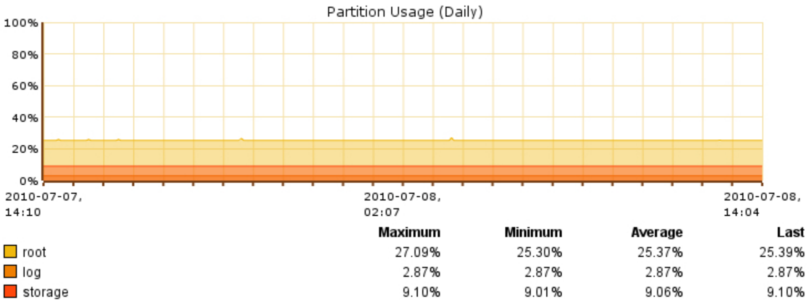


図166 レポーティング(Reporting):パーティション使用状況のヒストグラム

- **ルート(Root)**: ルートパーティションとは、Astaro Security Gatewayのルートディレクトリがあるパーティションです。このパーティションには、更新パッケージとバックアップも保存されます。
- **ログ(Log)**: ログパーティションとは、ログファイルとレポーティングデータが保存されるパーティションです。このパーティションの容量が不足している場合、*【ログおよびレポーティング(Logging & Reporting)】>>【ログ設定(Log Settings)】>>【ローカルログ(Local Logging)】*で設定を調整してください。
- **ストレージ(Storage)**: ストレージパーティションとは、プロキシサービスがデータを保存するパーティションであり、Webフィルタ用の画像、SMTPプロキシ用のメッセージ、隔離メールなどがここに保存されます。さらに、データベース、一時データ、設定ファイルも保存されます。

17.2.2ウィークリー

*【ハードウェア(Hardware)】>>【ウィークリー(Weekly)】*タブは、選択されたハードウェアコンポーネントに関する最近7日間の概要的な統計を示します。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.2.3マンスリー

*【ハードウェア(Hardware)】>>【マンスリー(Monthly)】*タブは、選択されたハードウェアコンポーネントに関する最近4週間の概要的な統計を示します。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.2.4イヤリー

*【ハードウェア(Hardware)】>>【イヤリー(Yearly)】*タブは、選択されたハードウェアコンポーネントに関する最近12か月の概要的な統計を示します。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.3ネットワーク使用状況

*【ログおよびレポーティング(Logging & Reporting)】>>【ネットワーク使用状況(Network Usage)】*メニューのタブには、さまざまな期間内にAstaro Security Gatewayの各インタフェースを通過したトラフィックに関する統計概観が表示されます。各チャートのデータは、次の単位を使用して示されます。

- u(マイクロ、$10e^{-6}$)
- m(ミリ、$10e^{-3}$)
- k(キロ、$10e^{3}$)
- M(メガ、$10e^{6}$)
- G(ギガ、$10e^{9}$)

$10e^{-18}$～$10e^{8}$の範囲内でスケールを変更可能です。

17.3.1デイリー

*【ネットワーク使用状況(Network Usage)】>>【デイリー(Daily)】*タブには、設定されている各インタフェースを通過するトラフィックに関する最近24時間の統計概観が表示されます。

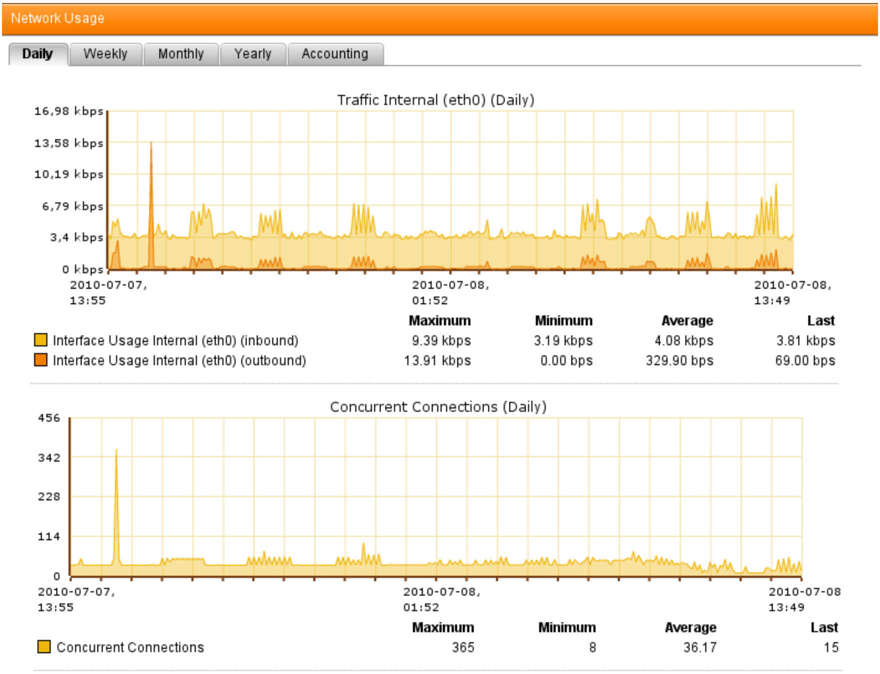


図167 レポーティング:イーサネットインタフェース使用状況のヒストグラム

各ヒストグラムには、次の2つのグラフが表示されます。

- **受信(Inbound)**: 該当インタフェースでの平均受信トラフィック(bps単位)。
- **送信(Outbound)**: 該当インタフェースでの平均送信トラフィック(bps単位)。

*【同時接続(Concurrent Connections)】*チャートは、同時接続の合計を示します。

17.3.2ウィークリー

*【ネットワーク使用状況(Network Usage)】>>【ウィークリー(Weekly)】*タブには、設定されている各インタフェースを通過するトラフィックに関する最近7日間の統計概観が表示されます。ヒ

ストグラムについては、「*デイリー*」のセクションを参照してください。

17.3.3マンスリー

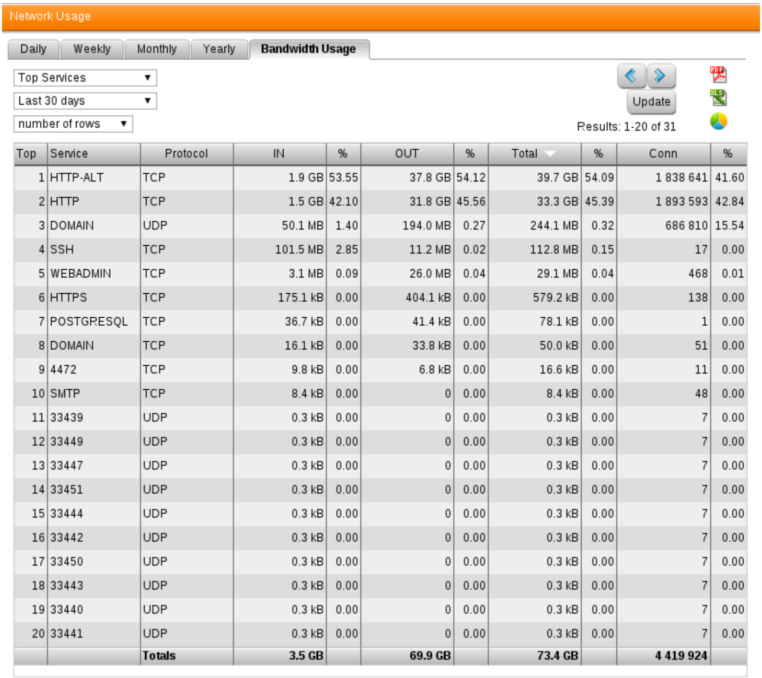
*【ネットワーク使用状況(Network Usage)】>>【マンスリー(Daily)】*タブには、設定されている各インタフェースを通過するトラフィックに関する最近4週間の統計概観が表示されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.3.4イヤリー

*【ネットワーク使用状況(Network Usage)】>>【イヤリー(Yearly)】*タブには、設定されている各インタフェースを通過するトラフィックに関する最近12か月の統計概観が表示されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.3.5帯域幅使用状況

*【ネットワーク使用状況(Network Usage)】>>【帯域幅使用状況(Bandwidth Usage)】*タブには、デバイスから転送されたネットワークトラフィック、デバイスに転送されたネットワークトラフィック、デバイスを経由して転送されたネットワークトラフィックについての包括的なデータが表示されます。



Top	Service	Protocol	IN	%	OUT	%	Total	%	Conn	%
1	HTTP-ALT	TCP	1.9 GB	53.55	37.8 GB	54.12	39.7 GB	54.09	1 838 641	41.60
2	HTTP	TCP	1.5 GB	42.10	31.8 GB	45.56	33.3 GB	45.39	1 893 593	42.84
3	DOMAIN	UDP	50.1 MB	1.40	194.0 MB	0.27	244.1 MB	0.32	686 810	15.54
4	SSH	TCP	101.5 MB	2.85	11.2 MB	0.02	112.8 MB	0.15	17	0.00
5	WEBADMIN	TCP	3.1 MB	0.09	26.0 MB	0.04	29.1 MB	0.04	468	0.01
6	HTTPS	TCP	175.1 kB	0.00	404.1 kB	0.00	579.2 kB	0.00	138	0.00
7	POSTGRESQL	TCP	36.7 kB	0.00	41.4 kB	0.00	78.1 kB	0.00	1	0.00
8	DOMAIN	TCP	16.1 kB	0.00	33.8 kB	0.00	50.0 kB	0.00	51	0.00
9	4472	TCP	9.8 kB	0.00	6.8 kB	0.00	16.6 kB	0.00	11	0.00
10	SMTP	TCP	8.4 kB	0.00	0	0.00	8.4 kB	0.00	48	0.00
11	33439	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
12	33449	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
13	33447	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
14	33451	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
15	33444	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
16	33442	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
17	33450	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
18	33443	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
19	33440	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
20	33441	UDP	0.3 kB	0.00	0	0.00	0.3 kB	0.00	7	0.00
		Totals	**3.5 GB**		**69.9 GB**		**73.4 GB**		**4 419 924**	

図168 レポーティング: 上位サービス順にソートされた帯域幅使用状況データ

結果の表の【*クライアント別(By Client)*】/【*サーバ別(By Server)*】ビューでIPまたはホスト名をクリックすると、これは自動的に【*クライアント別の上位サービス(Top Services By Client)*】ビューのフィルタとして使用されます。後でこれを【*サーバ別の上位サービス(Top Services by Server)*】ビューに切り替えることや、IP/ネットワークやネットワーク範囲(`192.168.1.0/24`、`10/8`など)を手動で指定して【*更新(Update)*】ボタンをクリックし、これらの設定を確定することができます。

【*サービス別(By Service)*】ビューでは、プロトコルとサービスをコンマで区切って入力することができます(*TCP,SMTP*、*UDP,6000*など)。プロトコルを指定しないと、TCPが使用されます(*HTTP*も有効です)。ページあたり20件を超える結果がある場合は、次ページ/前ページボタンを使用して前後のページに移動できます。

上位アプリケーション/上位アプリケーショングループ(Top Applications/Top Application Groups): アプリケーションコントロールがオフの場合、ネットワークトラフィックは「未分類」と表示されます。アプリケーションコントロールが有効な場合、ネットワークトラフィックはタイプで表示されます(例:「WebAdmin」、「NTP」、「facebook」)。アプリケーションコントロールに関する詳細は、「*Webセキュリティ*」>>「*アプリケーションコントロール*」の章を参照してください。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンがある場合はそれをクリックすると、表の上に円グラフが表示されます。

トラフィックのラベル*IN*と*OUT*は、視点に応じて変わります。プロキシモードで実行している場合、クライアントは(透過モードであっても)ASGでポート8080に接続するため、このクライアントから送信されたデータ(要求)は内部インタフェースにおいて*受信*トラフィックとなり、クライアント宛てに送信されたデータ(応答)は*送信*トラフィックとなります。

ヒント - 表の列見出しをクリックすると、すべてのデータを並べ替えることができます。たとえば、すべてのホストを受信トラフィック別にソートする場合、表の見出しで【*IN*】をクリックします。これにより、受信トラフィックが最も多く発生しているホストが先頭に表示されます。トラフィックのデータ量はキビバイト(KiB)およびメビバイト(MiB)単位で表示されます。いずれも、コンピュータの記憶容量を示す2の累乗単位です(例:1キビバイト = 2^{10}バイト = 1024バイト)。

17.4ネットワークセキュリティ

【*ログおよびレポーティング(Logging & Reporting)*】>>【*ネットワークセキュリティ(Network Security)*】メニューのタブには、Astaro Security Gatewayによって検出された関連ネットワークセキュリティイベントについての概要的な統計が表示されます。

17.4.1デイリー

【*ネットワークセキュリティ(Network Security)*】>>【*デイリー(Daily)*】タブは、次のイベントに関する過去24時間の統計概観を示します。

- ファイアウォール違反
- 侵入防御イベント

ファイアウォール違反(Firewall Violations): ドロップまたは拒否されたすべてのデータパケットは、ファイアウォール違反としてカウントされます。ファイアウォール違反の回数は、5分間の枠内で計算されます。

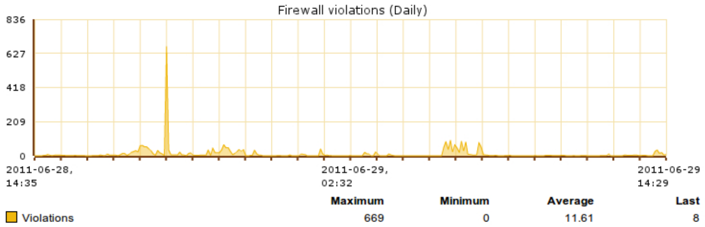


図169 レポーティング: ファイアウォール違反のヒストグラム(デイリー)

侵入防御イベント(Intrusion Prevention Events): すべてのチャートに、次の2つのグラフが表示されます。

- **アラートイベント(Alert Events)**: 侵入アラートを引き起こしたデータパケットの数。
- **ドロップイベント(Drop Events)**: 侵入防御システムによってドロップされたデータパケットの数。

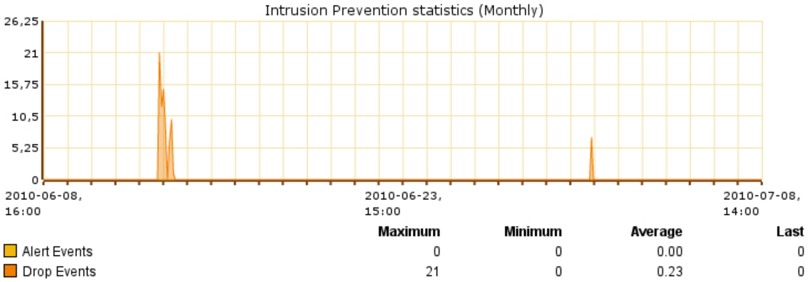


図170 レポーティング: 侵入防御イベントのヒストグラム(マンスリー)

17.4.2ウィークリー

*【ネットワークセキュリティ(Network Security)】>>【ウィークリー(Weekly)】*タブには、最近7日間以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.4.3マンスリー

*【ネットワークセキュリティ(Network Security)】>>【マンスリー(Monthly)】*タブには、最近4週間以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示

されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.4.4イヤリー

*【ネットワークセキュリティ(Network Security)】>>【イヤリー(Yearly)】*タブには、最近12か月以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.4.5ファイアウォール

*【ネットワークセキュリティ(Network Security)】>>【ファイアウォール(Firewall)】*タブには、ファイアウォールアクティビティに関する包括的なデータが、送信元IP、送信元ホスト、受信パケット数、サービス数に従って分類されて表示されます。

結果の表でIPまたはホスト名をクリックすると、*【上位サービス(Top Services)】*ビューのフィルタとして自動的に使用されます。IP/ネットワークやネットワーク範囲(`192.168.1.0/24`、`10/8`など)を手動で指定して、*【更新(Update)】*ボタンを押し、これらの設定を使用することができます。*【サービス別(By Service)】*ビューでは、プロトコルとサービスをコンマで区切って入力することができます(*TCP,SMTP*、*UDP,6000*など)。
ページあたり20件を超える結果がある場合は、次ページ/前ページボタンを使用して前後のページに移動できます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンがある場合はそれをクリックすると、表の上に円グラフが表示されます。

ヒント - 表の列見出しをクリックすると、すべてのデータを並べ替えることができます。たとえば、サービス数で表を並べ替える場合は、表見出しの*【サービス(Services)】*をクリックします。これにより、最も多くのサービスを要求した送信元IPがリストの一番先頭に表示されます。

17.4.6IPS

*【ネットワークセキュリティ(Network Security)】>>【IPS】*タブには、ネットワークでの侵入防御アクティビティに関する包括的なデータが表示されます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンがある場合はそれをクリックすると、表の上に円グラフが表示されます。

ヒント - 表の列見出しをクリックすると、すべてのデータを並べ替えることができます。たとえば、パケット数で表を並べ替える場合は、表見出しの【*パケット(Packet)*】をクリックします。すると、最も多くのパケットを要求した送信元IPが一番先頭に表示されます。

17.5Webセキュリティ

【*ログおよびレポーティング(Logging & Reporting)*】>>【*Webセキュリティ(Web Security)*】メニューのタブには、最もアクティブなWebユーザと最もよく表示されているWebサイトに関する概要的な統計が表示されます。

17.5.1Web使用状況レポート

【*ログおよびレポーティング(Logging & Reporting)*】>>【*Webセキュリティ(Web Security)*】>>【*Web使用状況レポート(Web Usage Report)*】ページは、ネットワークトラフィックやユーザのWeb使用状況を確認するための強力なツールです。一見するとこのページは非常に難解ですが、使用してみて結果を調べることから始めてみましょう。

ページ構成

ヘッダバー

まず、次の要素から構成されているヘッダバーがあります。

- **ホーム(Home)**: このアイコンを使用して、クリックやフィルタをすべてクリアして最初の状態に戻すことができます。
- **前へ(Forward)/次へ(Backward)**: これらのアイコンを使用して、変更や設定の履歴を前へ(または後ろへ)移動することができます。一般的なWebブラウザと同様に機能します。
- **利用可能なレポート(Available Reports)**: このドロップダウンリストには、保存されたレポート(もしあれば)を含む、利用可能なすべてのレポートタイプが含まれます。これはデフォルトで【*サイト(Sites)*】に設定されています。【*Web使用状況レポート(Web Usage Report)*】ページの結果テーブルは、このレポートタイプ設定に直接依存しています。

> **注 -** フィルタを使用してレポートを次々にクリックすると、【*利用可能なレポート(Available Reports)*】設定が自動的に変化するのを確認できます。これは常に、最新のレポート基準が反映されます。

標準(Standard): レポートタイプは5種類あります。詳細は以下を参照してください。

保存されたWebレポート(Saved Web Reports): ここでは、過去に作成した、保存されたWebレポートを選択できます。

- **削除(Delete)**: 保存されたWebレポートを削除するには、このアイコンをクリックします。標準レポートは削除できません。
- **保存(Save)**: 現在のビューを保存して、後日このビューに簡単にアクセスできるようにするには、このアイコンをクリックします。これは【*利用可能なレポート(Available Reports)*】ドロップダウンリストに保存されます。【*レポートの送信(Send Reports)*】チェックボックスにチェックを入れると、このレポートを送信すべきEメール受信者を1人以上入力することができます。また、保存されたレポートを定期的に受信することもできます。詳しくは「*スケジュールされたレポート*」を参照してください。

フィルタバー

次に、次の要素から構成されているフィルタバーがあります。

- **プラス(+)**: このアイコンをクリックして、追加のフィルタを作成します。詳細は以下を参照してください。
- **件数(Amount)**: ドロップダウンリストを使用して、テーブルに表示される結果を減らすことができます。結果を、上位10件、50件、100件の結果に制限することができます。
- **時間(Time)**: ドロップダウンリストを使用して、テーブルに表示される結果を、特定の時間枠内の結果に絞り込むか広げることができます。【*カスタム(Custom)*】タイムフレームを選択すると、独自の時間枠を指定できます。
- **部門(Departments)**: ドロップダウンリストを使用して、テーブルに表示される結果を、指定した部門に絞り込むことができます。部門は【*部門(Departments)*】ページで作成できます。

結果テーブル(Results Table)

最後に、結果テーブルがあります。ここに表示される結果は、第一に、選択したレポートタイプに依存し(【*利用可能なレポート(Available Reports)*】リストに常に反映)、第二に、定義したフィルタに依存します。

注 - 匿名化を有効にすると、ユーザは名前やIPアドレスで表示される代わりに、数値で列挙されます。

レポートタイプに応じて、テーブルには異なる情報が表示されます。

	ユーザ	**カテゴリ(Category):**	**サイト(Sites)**	**ドメイン(Domains):**	**URL**
#	✓	✓	✓	✓	✓
トラフィック(Traffic)	✓	✓	✓	✓	✓
%	✓	✓	✓	✓	✓
期間(Duration)	✓		✓		
ページ(Pages)	✓	✓	✓		
要求(Requests)	✓	✓	✓	✓	✓
カテゴリ(Categories)*					✓
アクション(Action)*					✓
理由(Reason)*					✓
情報(Info)*					✓

* = これらのセルをクリックして、情報をさらにドリルダウンできます。

#: 発声したトラフィックに関する順位。

トラフィック(Traffic): 発声したトラフィックのサイズ

%: トラフィック全体に対する割合。

期間(Duration): ユーザがWebサイトに滞在した時間

ページ(Pages): 要求されたページ数

要求(Requests): カテゴリ、サイト、ドメイン、またはURL別の要求数

カテゴリ(Categories): あるURLが属するすべてのカテゴリが表示されます。カテゴリが複数存在する場合、カテゴリをクリックすると小さいダイアログフィールドが開き、いずれかのカテゴリを選択できます。このカテゴリに基づいてフィルタが作成されます。

アクション(Action): Webサイトがクライアントに配信されたか(*配信済み(passed)*)、アプリケーションコントロールルールによってブロックされたかを表示します。

理由(Reason): Webサイト要求がブロックされた理由を表示します。例:ユーザがmsiファイルのダウンロードを試行し、ファイル転送を禁止するアプリケーションコントロールルールがあった場合、セルに理由が「msi」と表示されます。

情報(Info): 利用可能な場合、このセルにはWebサイト要求がブロックされた理由を示す追加情報が表示されます(例:ファイルダウンロードが拡張子に基づいてブロックされた場合、セルには「拡張子(extension)」と表示されます)。

フィルタの定義

フィルタは、結果テーブルに表示される情報をドリルダウンするために使用されます。2通りの定義方法があります。まず、フィルタバーの「+」アイコンをクリックするか、テーブルをクリックします。

「+」アイコンを使用する場合:フィルタバーで緑の「+」アイコンをクリックすると、フィールドが2つある小さいフィルタバーが表示されます。1番目のフィールドのドロップダウンリストを使用すると、レポートタイプを選択できます(「*カテゴリ(Category)*」など)。2番目のフィールドを使用すると、選択したレポートタイプの値を選択するか入力することができます(例:「*カテゴリ(Category)*」を選んだ場合、「*成人向けトピック(Adult Topics)*」など)。【*保存(Save)*】をクリックしてフィルタを保存し、結果テーブルに適用します。

テーブルを使用する場合:テーブルをクリックし、クリックしたアイテムに複数のレポートタイプがある場合は、【*レポート方向(Reporting Direction)*】が開きます。表示されたいずれかのオプションをフィルタ用に選択する必要があります。【*レポート方向(Reporting Direction)*】ウィンドウを閉じると、関連フィルタが作成され、フィルタバーに表示されます。結果テーブルに、新たにフィルタされた結果が表示されます。
例:【*Web使用状況レポート(Web Usage Report)*】のデフォルトレポートは【*サイト(Sites)*】です。結果テーブルで、任意の行をクリックします(例:「amazon.com」)。【*レポート方向(Reporting Direction)*】ウィンドウが開き、3つのオプションが提示されます。サイトのドメインに関する情報、サイトを訪問したユーザに関する情報、サイトが属するカテゴリに関する情報のいずれかを参照することができます。複数のユーザが「amazon.com」を訪問したことがわかりました。さらに詳細を確認するために、【*ユーザ(Users)*】ボックスをクリックします。ウィンドウが閉じます。ヘッダバーではレポートタイプが【*ユーザ(Users)*】に変わり、フィルタバーでは【*ユーザ(Users)*】の結果テーブルが選択したサイト(「amazon.com」)によってフィルタされたことを確認できます。したがって、テーブルにはこのサイトを訪問したすべてのユーザと、これらのセッションに関する追加情報が表示されます。

注 - 一部のテーブルセルには独自のフィルタがあるため(上の「*結果テーブル*」セクションでアスタリスク(*)の付いたアイテム)、クリックしたテーブル行によって結果が異なる場合があります。

17.5.2検索エンジンレポート

*【ログおよびレポーティング(Logging & Reporting)】>>【Webセキュリティ(Web Security)】>>【検索エンジンレポート(Search Engine Report)】*ページには、ユーザが使用している検索エンジンやユーザが行った検索に関する情報が表示されます。一見するとこのページは非常に難解ですが、使用してみて結果を調べることから始めてみましょう。

ページ構成

ヘッダバー

まず、次の要素から構成されているヘッダバーがあります。

- **ホーム(Home)**: このアイコンを使用して、クリックやフィルタをすべてクリアして最初の状態に戻すことができます。
- **前へ(Forward)/次へ(Backward)**: これらのアイコンを使用して、変更や設定の履歴を前へ(または後ろへ)移動することができます。一般的なWebブラウザと同様に機能します。
- **利用可能なレポート(Available Reports)**: このドロップダウンリストには、保存されたレポート(もしあれば)を含む、利用可能なすべてのレポートタイプが含まれます。これはデフォルトで*【検索(Searches)】*に設定されています。*【検索エンジンレポート(Search Engine Report)】*ページの結果テーブルは、このレポートタイプ設定に直接依存しています。

  注 - フィルタを使用してレポートを次々にクリックすると、*【利用可能なレポート(Available Reports)】*設定が自動的に変化するのを確認できます。これは常に、最新のレポート基準が反映されます。

  標準(Standard): レポートタイプは3種類あります。詳細は以下を参照してください。

  保存された検索エンジンレポート(Saved Search Engine Reports): ここでは、過去に作成した、保存された検索エンジンレポートを選択できます。
- **削除(Delete)**: 保存された検索エンジンレポートを削除するには、このアイコンをクリックします。標準レポートは削除できません。

- **保存(Save)**: 現在のビューを保存して、後日このビューに簡単にアクセスできるようにするには、このアイコンをクリックします。これは【*利用可能なレポート(Available Reports)*】ドロップダウンリストに保存されます。【*レポートの送信(Send Reports)*】チェックボックスにチェックを入れると、このレポートを送信すべきEメール受信者を1人以上入力することができます。また、保存されたレポートを定期的に受信することもできます。詳しくは「*スケジュールされたレポート*」を参照してください。

フィルタバー

次に、次の要素から構成されているフィルタバーがあります。

- **プラス(+)**: このアイコンをクリックして、追加のフィルタを作成します。詳細は以下を参照してください。
- **件数(Amount)**: ドロップダウンリストを使用して、テーブルに表示される結果を減らすことができます。結果を、上位10件、50件、100件の結果に制限することができます。
- **時間(Time)**: ドロップダウンリストを使用して、テーブルに表示される結果を、特定の時間枠内の結果に絞り込むか広げることができます。【*カスタム(Custom)*】タイムフレームを選択すると、独自の時間枠を指定できます。
- **部門(Departments)**: ドロップダウンリストを使用して、テーブルに表示される結果を、指定した部門に絞り込むことができます。部門は【*部門(Departments)*】ページで作成できます。

結果テーブル(Results Table)

最後に、結果テーブルがあります。ここに表示される結果は、第一に、選択したレポートタイプに依存し(【*利用可能なレポート(Available Reports)*】リストに常に反映)、第二に、定義したフィルタに依存します。次のレポートタイプを使用できます。

- **検索(Searches)**: ユーザが使用した検索文字列を表示します。
- **検索エンジン(Search Engines)**: ユーザが使用した検索エンジンを表示します。
- **ユーザの検索(Users Searches)**: 検索を行ったユーザを表示します。

注 - 匿名化を有効にすると、ユーザは名前やIPアドレスで表示される代わりに、数値で列挙されます。

それぞれのレポートタイプに対して、テーブルには以下の情報が表示されます。

#: 頻度に関する順位。

要求(Requests): 検索文字列、検索エンジン、ユーザ別の要求回数。

%: 検索全体に対する割合。

フィルタの定義

フィルタは、結果テーブルに表示される情報をドリルダウンするために使用されます。2通りの定義方法があります。まず、フィルタバーの「＋」アイコンをクリックするか、テーブルをクリックします。

「＋」アイコンを使用する場合：フィルタバーで緑の「＋」アイコンをクリックすると、フィールドが2つある小さいフィルタバーが表示されます。1番目のフィールドのドロップダウンリストを使用すると、レポートタイプを選択できます（「*検索エンジン(Search Engine)*」など）。2番目のフィールドを使用すると、選択したレポートタイプの値を選択するか入力することができます（例：「*検索エンジン(Search Engine)*」を選んだ場合、「*Google(google.com)*」など）。【*保存(Save)*】をクリックしてフィルタを保存し、結果テーブルに適用します。

テーブルを使用する場合：テーブルをクリックし、クリックしたアイテムに複数のレポートタイプがある場合は、【*レポート方向(Reporting Direction)*】が開きます。表示されたいずれかのオプションをフィルタ用に選択する必要があります。【*レポート方向(Reporting Direction)*】ウィンドウを閉じると、関連フィルタが作成され、フィルタバーに表示されます。結果テーブルに、新たにフィルタされた結果が表示されます。
例：【*検索エンジンレポート(Search Engine Report)*】のデフォルトレポートは【*検索(Searches)*】です。結果テーブルで、任意の行をクリックします（例：「天気」）。【*レポート方向(Reporting Direction)*】ウィンドウが開き、2つのオプションが提示されます。検索に対して使用された検索エンジンに関する情報を表示するか（【*検索エンジン(Search Engines)*】）、この文字列を検索したユーザに関する情報を表示します（【*ユーザ検索(Users Searches)*】）。複数のユーザが「天気」について検索したことがわかりました。さらに詳細を確認するために、【*ユーザ検索(Users Searches)*】ボックスをクリックします。ウィンドウが閉じます。ヘッダバーでレポートタイプが【*ユーザ検索(Users Searches)*】に変わり、フィルタバーで【*ユーザ検索(Users Searches)*】の結果テーブルが選択した検索文字列（「天気」）によってフィルタされたことを確認できます。したがって、テーブルには「天気」について検索したすべてのユーザと、これらの検索に関する追加情報が表示されます。

注 - 一部のテーブルセルには独自のフィルタがあるため（上の「*結果テーブル*」セクションでアスタリスク（*）の付いたアイテム）、クリックしたテーブル行によって結果が異なる場合があります。

17.5.3部門

【*ログおよびレポーティング(Logging & Reporting)*】>>【*Webセキュリティ(Web Security)*】>>【*部門(Departments)*】ページでは、ユーザまたはホストおよびネットワークを仮

想部門にグループ化することができます。次に、これらの部門を使用してWeb使用状況レポートや検索エンジンレポートをフィルタすることができます。

部門を作成するには、次の手順に従います。

1. ***【部門(Departments)】タブで、【部門の追加(Add Department)】をクリックします。***
   *【新規部門の追加(Add New Department)】*ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前(Name):部門を説明する名前を入力してください。
3. **ユーザまたはホスト/ネットワークを追加します。**
   部門の定義には、ユーザとホスト/ネットワークのいずれかしか含めることができず、両方を同時に含めることはできません。
   - **ユーザ(Users)**: この部門に加えるユーザを1人以上ボックスに追加します。
   - **ホスト/ネットワーク(Hosts/Networks)**: この部門に加えるホストまたはネットワークを1つ以上ボックスに追加します。

   コメント(Comment)(オプション):説明などの情報を追加します。
4. ***【保存(Save)】をクリックします。***

   新しい部門が*【部門(Departments)】*リストに表示されます。

部門を編集、削除、または複製するには、対応するボタンをクリックします。

部門の使用について詳しくは、「*Web使用状況レポート*」と「*検索エンジンレポート*」のセクションを参照してください。

17.5.4スケジュールされたレポート

*【ログおよびレポーティング(Logging & Reporting)】>>【Webセキュリティ(Web Security)】>>【スケジュールされたレポート(Scheduled Reports)】*ページでは、定期的にEメールで送信したい保存済みレポートを定義することができます。スケジュールされたレポートを作成するためには、あらかじめ保存済みのレポートが少なくとも1つ必要です(レポートの保存については、「*Web使用状況レポート*」または「*検索エンジンレポート*」のセクションを参照)。

スケジュールされたレポートを作成するには、次の手順に従います。

1. ***【スケジュールされたレポート(Scheduled Reports)】タブで、【スケジュールされたレポートの追加(Add Scheduled Report)】をクリックします。***

*【新しいスケジュールされたレポートの追加(Add New Scheduled Report)】*ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(Name):スケジュールされたレポートを説明する名前を入力してください。

   間隔(Interval): ドロップダウンリストから、レポートを送信する間隔を選択します。

   レポート(Reports): 保存されたすべてのレポートがここに表示されます。選択した間隔で送信する各レポートの前にあるチェックボックスにチェックを入れてください。

   受信者(Recipients): 選択したレポートを受信する受信者をボックスに追加します。インポートボタンを使用して受信者のリストを追加することができます。

   コメント(Comment)(オプション):説明などの情報を追加します。

3. ***【保存(Save)】*をクリックします。**

   新しいスケジュールされたレポートが*【スケジュールされたレポート(Scheduled Reports)】*リストに表示されます。

部門を編集、削除、または複製するには、対応するボタンをクリックします。スケジュールされたレポート自体を削除せずにレポートの送信を無効化するには、レポートのステータスアイコンを使用します。

17.5.5アプリケーションコントロール

*【ログおよびレポーティング(Logging& Reporting)】>>【Webセキュリティ(Web Security)】>>【アプリケーションコントロール(Application Control)】*ページには、様々な期間における最もアクティブな送信元、最も訪問が頻繁な宛先、最も人気の高いアプリケーションについての総合的な統計が表示されます。変更した場合は、必ず*【更新(Update)】*ボタンをクリックして確定してください。ページあたり20件を超える結果がある場合は、次ページ/前ページボタンを使用して前後のページに移動できます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンがある場合はそれをクリックすると、表の上に円グラフが表示されます。

ヒント - 表の列見出しをクリックすると、すべてのデータを並べ替えることができます。たとえば、送受信パケット数ですべての送信元を並べ替える場合は、表見出しの*【パケット(Packets)】*をクリックします。これにより、最も多くのパケットを送受信した送信元がリストの一番上に表示されます。

最もアクティブな送信元はすぐには表に表示されず、セッションタイムアウトの発生後に表示されます。たとえば、特定クライアント(ユーザ名またはIPアドレス)が5分間Webサーフィンを停止したとします。この場合、ASGはこのサーフィンセッションを「デッド(dead)」と判断し、最もアクティブな送信元リストに表示する前にデータベースに送ります。

さらに、*【アプリケーション別(By Application)】*あるいは*【送信元別(By Source)】*を使用したレポートも選択できます。続いて、フィルタフィールドが表示されます。ここに、求めるアプリケーションや送信元を入力し、*【更新(Update)】*をクリックして設定を確認する必要があります。表には、指定したアプリケーションまたは送信元でフィルタされた結果が表示されます(もしあれば)。パーセント記号(%)をワイルドカードとして使用できます。キーワード末尾にパーセント記号を付けた場合は、完全一致または部分一致を検索するようにAstaro Security Gatewayに指示することになります。フィルタフィールドでは大文字と小文字が区別されます。例:*【アプリケーション(Application)】*フィールドに「Google%」と入力すると、表には「Google Safe Browsing」、「Google Analytics」、「Google」などが表示されますが、「google」は表示されません。

17.5.6非匿名化

【Webセキュリティ(Web Security)】>>*【非匿名化(Deanonymization)】*タブは、匿名化が有効になっている場合のみアクセス可能です(*「ログおよびレポーティング」*>>*「レポーティング設定」*>>*「匿名化」*を参照)。

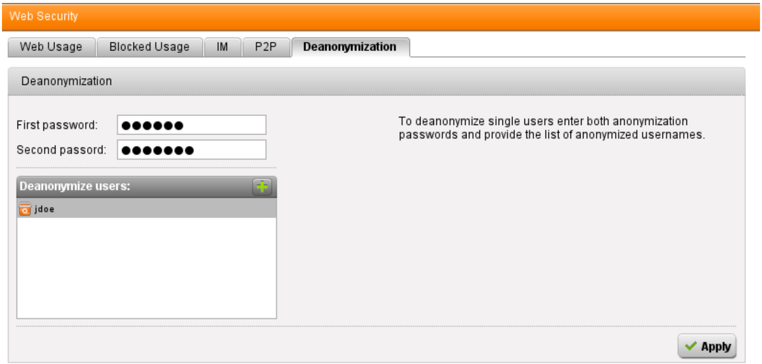


図171 レポーティング:シングルユーザの非匿名化

ここでは、Webセキュリティレポートに関する特定ユーザの匿名化をやめることができます。次の手順で実行します。

1. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。
2. **非匿名化にするユーザを追加します。**
   *【ユーザの非匿名化(Deanonymize Users)】*ボックスに、非匿名にするユーザのユーザ名を追加します。
3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

17.6メールセキュリティ

*【ログおよびレポーティング(Logging & Reporting)】>>【メールセキュリティ(Mail Security)】*メニューのタブには、メールフロー、メール使用状況、およびメールセキュリティについての概要的な統計が表示されます。

17.6.1使用状況グラフ

*【メールセキュリティ(Mail Security)】>>【使用状況グラフ(Usage Graphs)】*タブには、さまざまな時間枠内にASGを通過したメールフローの概要的な統計が表示されます。

- デイリー
- ウィークリー
- マンスリー
- イヤリー

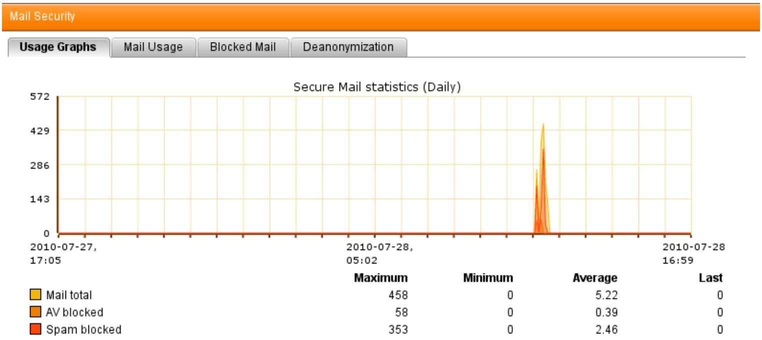


図172 レポーティング: メールフローのヒストグラム

17.6.2メール使用状況

*【メールセキュリティ(Mail Security)】>>【メール使用状況(Mail Usage)】*タブには、さまざまな時間枠内で最もアクティブに使用されたEメールアドレスやアドレスドメインに関する包括的な統計が表示されます。変更した場合は、必ず*【更新(Update)】*ボタンをクリックして確定してください。ページあたり20件を超える結果がある場合は、次ページ/前ページボタンを使用して前後のページに移動できます。

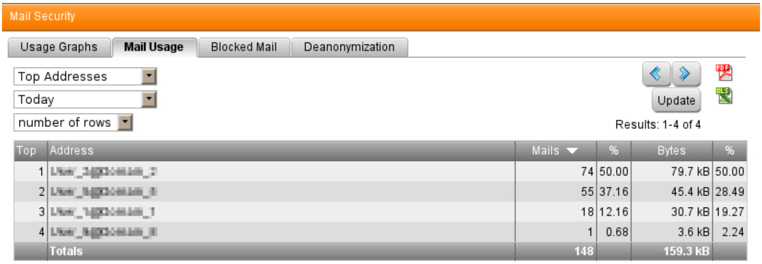


図173 レポーティング: 最もアクティブなEメールアドレスのランキング

17.6.3ブロックされたメール

*【メールセキュリティ(Mail Security)】>>【ブロックされたメール(Blocked Mail)】*タブには、アンチウイルスおよびアンチスパムによってブロックされたすべてのEメール要求に関する包括的な統計が表示されます。変更した場合は、必ず*【更新(Update)】*ボタンをクリックして確定してください。ページあたり20件を超える結果がある場合は、次ページ/前ページボタンを使用して前後のページに移動できます。

17.6.4非匿名化

*【メールセキュリティ(Mail Security)】>>【非匿名化(Deanonymization)】*タブは、匿名化が有効になっている場合のみアクセス可能です(*「ログおよびレポーティング(Logging & Reporting)」>>「レポーティング設定」>>「*<u>匿名化</u>」を参照)。

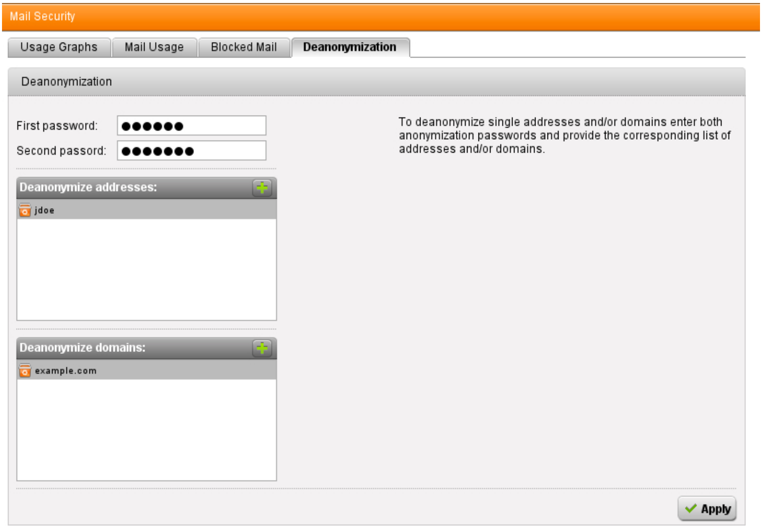


図174 レポーティング:Eメールアドレスとドメインの非匿名化

ここでは、メールセキュリティレポートで特定のEメールアドレスやドメインの匿名化を中止することができます。次の手順で実行します。

1. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。

2. **次の設定を行います。**
   アドレスの非匿名化(Deanonymize Addresses): 非匿名化するEメールアドレスを追加します。

   ドメインの非匿名化(Deanonymize Domains): 非匿名化するドメインを追加します。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

   指定したEメールアドレスとドメインはレポートに表示されるようになります。

17.7リモートアクセス

*【ログおよびレポーティング(Logging & Reporting)】>>【リモートアクセス(Remote Access)】*メニューのタブは、リモートアクセスアクティビティおよびセッション情報に関する全体的な統計を提供します。

17.7.1アクティビティ

*【リモートアクセス(Remote Access)】>>【アクティビティ(Activity)】*タブは、さまざまな期間についてASG IPsec、SSL VPN、PPTP、およびL2TPのリモートアクセスに関する統計概要を提供します。

- デイリー
- ウィークリー
- マンスリー
- イヤリー

期間を選択(Select Timeframe): ドロップダウンリストを使用して、レポート期間を選択します。ページは自動的にリロード(再読み込み)されます。

17.7.2セッション

*【リモートアクセス(Remote Access)】>>【セッション(Session)】*タブは、さまざまな時間範囲について、完了したセッション、失敗したログイン、および現在のユーザに関する包括的な統計を提供します。

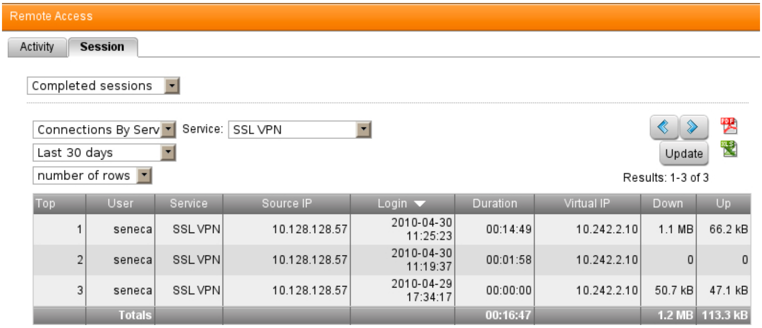


図175 レポーティング：最後の30日間の完了したセッション接続

表のデータはフィルタできます。表のヘッダセルをクリックすると、最もすばやくフィルタできます。もう1つの方法は、2番目のドロップダウンリストからフィルタを選択し、フィルタ引数を入力して*【更新(Update)】*ボタンをクリックする方法です。

最初のドロップダウンリストで選択したセッションに応じて、以下のフィルタを使用できます。

- **サービス毎(By Service)**：*現在のユーザ(Current Users)、完了したセッション(Completed Sessions)、失敗したログイン(Failed Logins)*
- **ユーザ毎(By User)**：*現在のユーザ(Current Users)、完了したセッション(Completed Sessions)*
- **送信元IPアドレス毎(By Source IP Address)**：*現在のユーザ(Current Users)、完了したセッション(Completed Sessions)*
- **仮想IPアドレス毎(By Virtual IP Address)**：*現在のユーザ(Current Users)、完了したセッション(Completed Sessions)、失敗したログイン(Failed Logins)*

ページあたり20件を超える結果がある場合は、次ページ/前ページボタンを使用して前後のページに移動できます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンがある場合はそれをクリックすると、表の上に円グラフが表示されます。

ヒント - 表の列見出しをクリックすると、すべてのデータを並べ替えることができます。たとえば、サービス別に表を並び替える場合は、表見出しの*【サービス(Service)】*をクリックします。これで、表はサービス別にアルファベット順に並び替えられます。

17.8Webアプリケーションファイアウォール

*【ログおよびレポーティング(Logging & Reporting)】>>【Webアプリケーションファイアウォール(Web Application Firewall)】*メニューのタブは、Webサーバの要求、警告、アラートに関する全体的な統計を提供します。

17.8.1使用状況グラフ

*【Webアプリケーションファイアウォール(Web Application Firewall)】>>【使用状況グラフ(Usage Graphs)】*タブは、さまざまな時間枠内にASGで発生したWebサーバの要求、警告、アラートに関する全体的な統計を提供します。

- デイリー
- ウィークリー
- マンスリー
- イヤリー

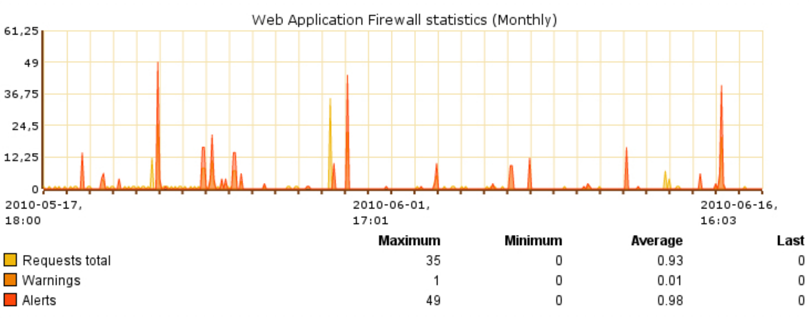


図176 レポーティング:Webアプリケーションファイアウォールのマイスリーアクティビティのヒストグラム

17.8.2詳細

*【Webアプリケーションファイアウォール(Web Application Firewall)】>>【詳細(Details)】*タブには、さまざまな時間枠内で最もアクティブだったクライアント、仮想ホスト、バックエンド、応答コード、および様々な攻撃に関する包括的な統計が表示されます。変更した場合は、必ず*【更*

新(Update)】ボタンをクリックして確定してください。ページあたり20件を超える結果がある場合は、次ページ/前ページボタンを使用して前後のページに移動できます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、円グラフのアイコンがある場合はそれをクリックすると、表の上に円グラフが表示されます。

ヒント - 表の列見出しをクリックすると、すべてのデータを並べ替えることができます。

17.9エグゼクティブレポート

*【ログ(Logging)】&【レポーティング(Reporting)】>>【エグゼクティブレポート(Executive Report)】*メニューでは、各サービスのネットワーク使用状況を表示するために重要なレポーティングデータをグラフィカルな形式にまとめることができます。

17.9.1レポートを見る[View Report]

*【ログおよびレポーティング(Logging & Reporting)】>>【エグゼクティブレポート(Executive Report)】>>【レポートを見る(View Report)】*タブでは、*【レポーティング(Reporting)】*メニューのタブとページにある個々のレポートに基づいて、完全なエグゼクティブレポートを作成することができます。エグゼクティブレポートを表示するウィンドウを開くには、*【レポートを作成(Generate Report Now)】*ボタンをクリックします。

17.9.2アーカイブエグゼクティブレポート[Archived Executive Reports]

*【エグゼクティブレポート(Executive Report)】>>【アーカイブエグゼクティブレポート(Archived Executive Reports)】*タブには、アーカイブされたすべてのエグゼクティブレポートの概要が表示されます。*【設定(Configuration)】*タブでアーカイブが選択されているエグゼクティブレポートのみがアーカイブされます。

17.9.3設定

*【エグゼクティブレポート(Executive Report)】>>【設定(Configuration)】*タブでは、エグゼクティブレポートの設定を行うことができます。

エグゼクティブレポートの期間を選択します。レポートは、デイリー、ウィークリー、マンスリーベースで作成することができます。*【ウィークリー(Weekly)】*を選択した場合、エグゼクティブレポートがデータの収集を開始する曜日も選択できます。

さらに、エグゼクティブレポートの受信者のメールアドレスを入力します。異なる期間に対して異なるメールアドレスを設定することができます。

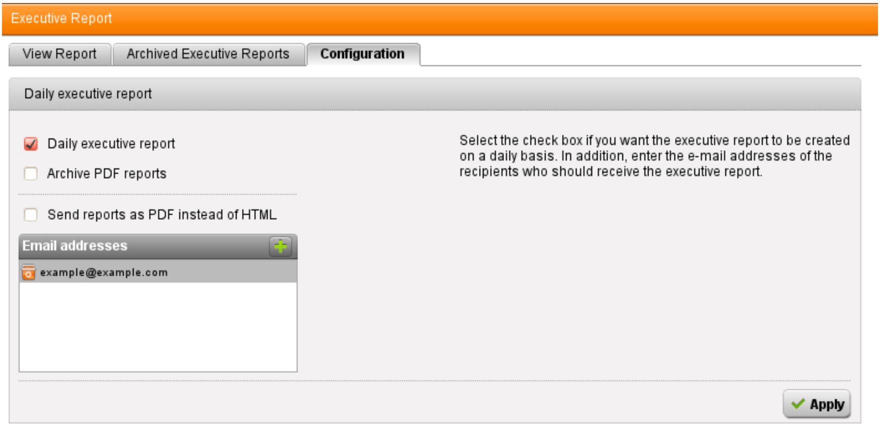


図177 レポーティング(Reporting):デイリーエグゼクティブレポートの設定

17.10ログ設定

*【ログおよびレポーティング(Logging & Reporting)】>>【ログ設定(Log Settings)】*メニューで、ローカルおよびリモートログの基本的な設定を構成できます。

17.10.1ローカルログ

*【ログおよびレポーティング(Logging & Reporting)】>>【ログ設定(Log Settings)】>>【ローカルログ(Local Logging)】*タブで、ローカルログの設定を行うことができます。デフォルトではローカルログは有効になっています。

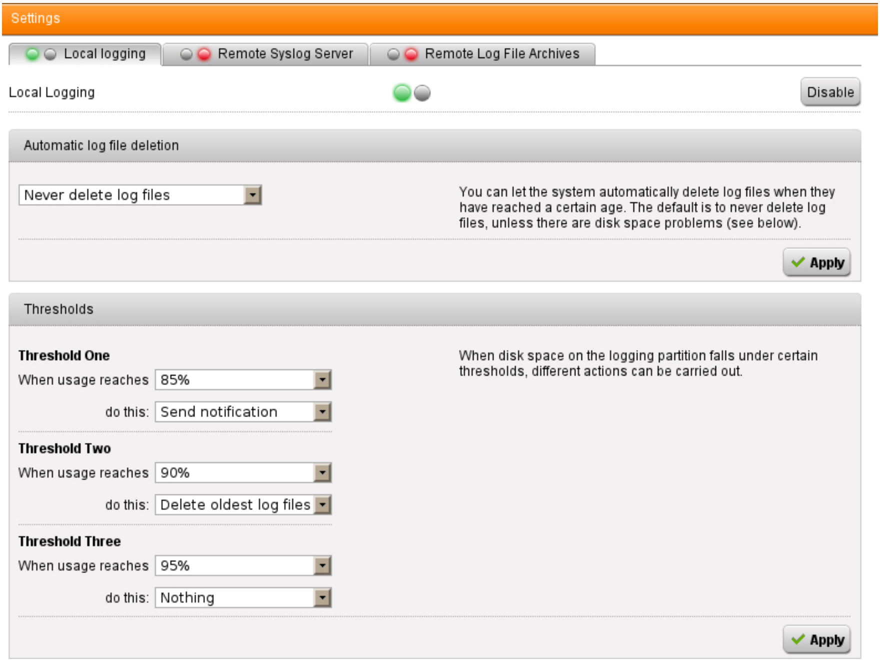


図178 ログ:ローカルログの有効化

ただし、ローカルログが無効になっている場合は、以下の手順で有効にできます。

1. ***【ローカルログ(Local Logging)】タブでローカルログを有効にします。***
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンが緑色に変わり、このタブ内のエリアが編集可能になります。

2. **ログファイルを削除する時間枠を選択します。**
   ドロップダウンリストから、ログファイルに自動的に適用するアクションを選択します。デフォルトでは、*【ログファイルを削除しない(Never delete log files)】*が選択されています。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

しきい値(Thresholds)

ここでローカルログのしきい値を定義できます。しきい値は、この値に達した場合に実行される特定のアクションに結び付けられます。次の作業を実行できます。

- **なし(Nothing)**: 何も起こりません。
- **通知を送信(Send Notification)**:しきい値に達したことを管理者に伝える通知を送信します。
- **一番古いログファイルを削除(Delete Oldest Logfiles)**:残りの量が設定したしきい値より下になるまで、あるいはログファイルのアーカイブが空になるまで、一番古いログファイルが削除されます。さらに、そのアクションの通知が管理者に送信されます。
- **システムをシャットダウン(Shutdown System)**:システムがシャットダウンします。そのアクションの通知が管理者に送信されます。
  システムをシャットダウンする場合は、管理者はローカルログの設定を変更し、ログファイルの削除を設定するか、あるいはログファイルを手動で移動/削除する必要があります。システムシャットダウンの理由が持続する場合は、次回のログ消去プロセスの実行時(毎日午前12:00つまり真夜中に実施)にシステムは再び自らをシャットダウンします。

設定を保存するには【*適用(Apply)*】をクリックします。

17.10.2リモートSyslogサーバ

【*ログおよびレポーティング(Logging & Reporting)*】>>【*ログ設定(Log Settings)*】>>【*リモートSyslogサーバ(Remote Syslog Server)*】タブで、リモートログの設定を行うことができます。この機能により、ゲートウェイから他のホストにログメッセージを転送できます。これは、ホストを使用していくつかのゲートウェイからログ情報を収集するネットワークで特に役立ちます。選択したホストでは、Syslogプロトコル互換のログデーモンを実行する必要があります。

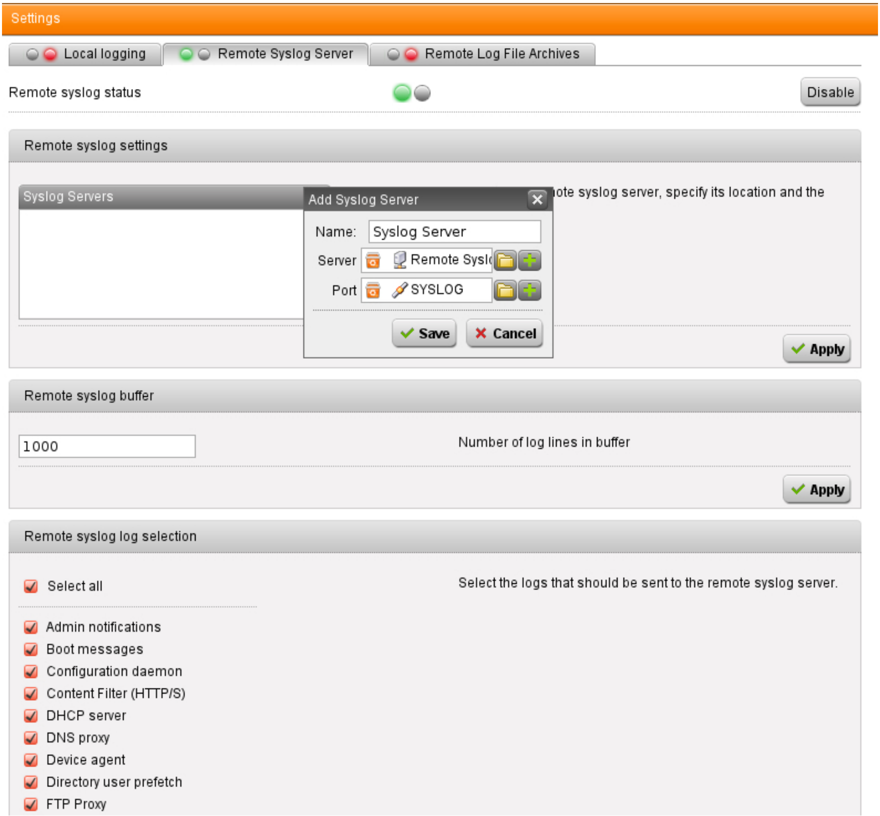


図179 ログ: リモートSyslogサーバの設定

リモートsyslogサーバを設定するには、以下の手順に従います。

1. ***【リモートSyslogサーバ(Remote Syslog Server)】タブでリモートsyslogを有効にします。***

   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり、*【リモートSyslog設定(Remote Syslog Settings)】*エリアが編集可能になります。

2. ***【Syslogサーバ(Syslog Servers)】ボックスの「+」アイコンをクリックしてサーバを作成します。***

   *【Syslogサーバの追加(Add Syslog Server)】*ダイアログボックスが開きます。

3. **次の設定を行います。**
   名前(Name): リモートsyslogサーバを説明する名前を入力します。

   サーバ(Server): ゲートウェイからログデータを受信する必要があるホストを追加または選択します。

   > **警告 -**ゲートウェイ自体のインターフェースをリモートsyslogホストとして使用しないでください。これを行うと、ログループになります。

   ポート(Port): 接続に使用するポートを追加または選択します。

4. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

リモートSyslogバッファ(Remote Syslog Buffer)

このエリアで、リモートsyslogのバッファサイズを変更できます。バッファサイズはバッファに保持されるログの行数です。デフォルトは1000です。設定を保存するには*【適用(Apply)】*をクリックします。

リモートSyslogログの選択(Remote Syslog Log Selection)

このエリアはリモートsyslogが有効なときのみ編集できます。syslogサーバに送信するログのチェックボックスにチェックを入れてください。*【すべてを選択(Select All)】*オプションを選択すると、一度にすべてのログを選択することができます。設定を保存するには*【適用(Apply)】*をクリックします。

17.10.3リモートログファイルアーカイブ

*【ログおよびレポーティング(Logging & Reporting)】>>【ログ設定(Log Settings)】>>【リモートログファイルアーカイブ(Remote Logfile Archives)】*タブで、ログファイルのリモートアーカイブを設定することができます。リモートログファイルのアーカイブを有効にすると、これまでのログファイルは1つのファイルに集約・圧縮され、リモートログファイルのストレージに転送されます。ドロップダウンリストで転送方法を選択できます。

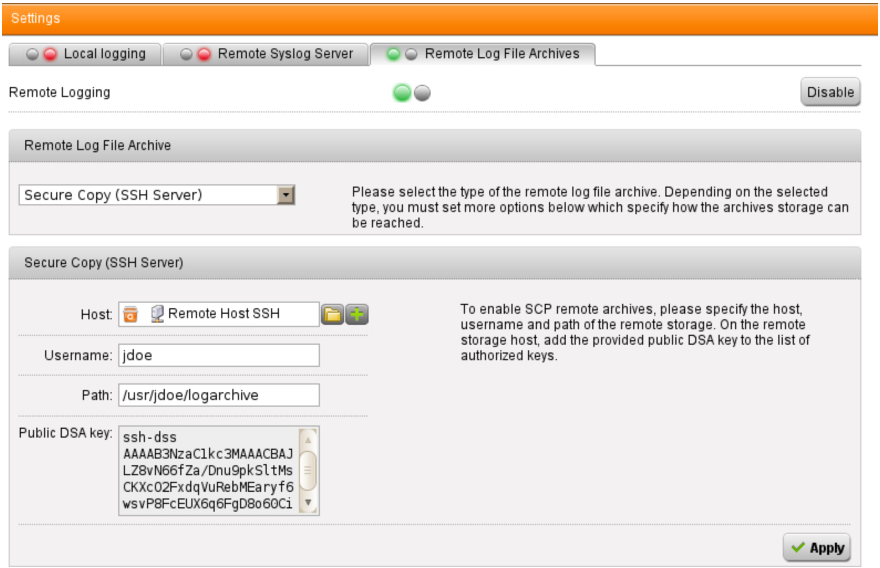


図180 ログ:リモートログファイルアーカイブの設定

リモートログファイルのアーカイブを設定するには、以下の手順に従います。

1. ***リモートログファイルアーカイブ(Remote Log File Archives)*機能を有効にします。**
   ステータスアイコンまたは【*有効(Enable)*】ボタンをクリックします。

   ステータスアイコンがアンバー色に変わり、【*リモートログファイルアーカイブ(Remote Logfile Archive)*】エリアが編集可能になります。

2. **ログファイルのアーカイブ方式を選択します。**
   ドロップダウンリストで、希望のアーカイブ方式を選択します。選択した方式に応じて、各アーカイブ方式に関連する設定オプションが下に表示されます。以下のアーカイブ方式から選択できます。

   - **FTPサーバ(FTP Server)**:*FTP(ファイル転送プロトコル)*方式では、以下のパラメータを設定する必要があります。
     - **ホスト(Host)**:FTPサーバのホストの定義。
     - **サービス(Service)**: サーバがリスンするTCPポート。
     - **ユーザ名(Username)**:FTPサーバアカウントのユーザ名。
     - **パスワード(Password)**:FTPサーバアカウントのパスワード。
     - **パス(Path)**:ログファイルが保存されているリモート(相対)パス。

- **SMB(CIFS)シェア(SMB(CIFS)Share)**: SMB方式では、以下のパラメータの設定が必要です。
  - **ホスト(Host)**: SMBサーバのホストの定義。
  - **ユーザ名(Username)**: SMBアカウントのユーザ名。
  - **パスワード(Password)**: SMBアカウントのパスワード。

    セキュリティに関する注記 - パスワードは設定ファイルにプレーンテキストで保存されます。したがって、このログに固有のユーザ/パスワードの組み合わせを作成することをお勧めします。

  - **共有(Share)**: SMB共有名。ログファイルの転送先のパスまたはネットワーク共有情報を入力します(例: `/logs/logfile_archive`)。
  - **ワークグループ/ドメイン(Workgroup/Domain)** ログファイルのアーカイブを入れるワークグループまたはドメインを入力します。
- **セキュアコピー(SSHサーバ)(Secure Copy(SSH Server))**: SCP方式を使用するには、公開SSH DSA鍵を、お使いのSCPサーバの承認済み鍵に追加する必要があります。Linuxシステムでは、SSH DSA鍵をカット&ペーストして、設定されたユーザアカウントの`~/.ssh/authorized_keys`ファイルに追加できます。インストール時にAstaro Security Gateway によって新しいSSHDSA 鍵が作成されます。セキュリティ上の理由から、このSSH DSA鍵はバックアップには含まれません。したがって、新規またはバックアップのインストール後に、新しいSSH DSA鍵をリモートサーバに保存して、ログファイルのアーカイブをSCPサーバに安全にコピーできるようにする必要があります。
  SCP方式には以下の設定が必要です。
  - **ホスト(Host)**: SCPサーバのホストの定義。
  - **ユーザ名(Username)**: SCPサーバアカウントのユーザ名。
  - **パス(Path)**: ログファイルの保存先の(完全な)リモートパス。
  - **公開DSA鍵(Public DSA Key)**: リモートストレージホスト上で、提供された公開DSA鍵を承認済み鍵のリストに追加します。
- **Eメールで送信(Send by E-mail)**: ログファイルのアーカイブをEメールで送信するために、有効なEメールアドレスを入力します。

3. ***【適用(Apply)】*をクリックします。**
   設定が保存されます。

転送が失敗すると、アーカイブはゲートウェイに残ります。それぞれのログ削除プロセス時に、ゲートウェイは残りすべてのアーカイブを配信しようと試みます。

17.11レポーティング設定

*【ログおよびレポーティング(Logging & Reporting)】>>【レポーティング設定(Reporting Settings)】*メニューで、レポーティングの特定機能の有効化/無効化やデータ保持時間/量の設定といったレポーティング機能の設定を行うことができます。さらに、プライバシ保護を強化するためにデータを匿名にすることができます。

17.11.1設定

*【設定(Settings)】*タブで、レポートアクションおよびレポートデータが自動的に削除されるまでのシステムでの保持期間を定義できます。以下のレポートトピックを設定できます。

- アカウンティング
- アプリケーションコントロール
- 認証
- メールセキュリティ
- ファイアウォール
- IPS
- リモートアクセス
- Webアプリケーションファイアウォール
- Webセキュリティ

左側のチェックボックスを使用して、特定トピックに関するレポートを有効/無効にします。デフォルトでは、すべてのレポートトピックが有効になっています。

右側のドロップダウンリストを使用して、レポートデータの保持期間を設定します。

注 - 不要なレポートを無効にすることで、マシンの基本的な負荷を減らし、パフォーマンスのボトルネックを削減できます。レポートの保持期間はできるだけ短く設定してください。保存データの量が多いと基本的な負荷が高くなり、動的なレポートページの応答性を低下させます。

このタブの設定は、ログファイルアーカイブへは影響しません。

Webセキュリティレポート詳細レベル

このセクションでは、Webセキュリティレポートの詳細レベルを定義することができます。詳細レベルを高くすると、メモリの使用量とシステム負荷が目に見えて増加するため、必要でない限りは、詳細レベルを低くしてください。

以下の詳細レベルを設定できます。

- **ドメインのみ(Domain only)**: レポートには、URLのトップレベルドメインとセカンドレベルドメイン(例:`example.com`)が表示されます。サードレベルドメインは、強制すると表示されます(例:`example.co.uk`)。
- **フルドメイン(Full domain)**: レポートには、フルドメインが表示されます(例:`www.example.com`、`shop.example.com`)。
- **URLの1レベル(1 level of URL)**: レポートには、URLの最初の(仮想)ディレクトリが追加で表示されます(例:`www.example.com/en/`)。
- **URLの2レベル(2 levels of URL)**: レポートには、URLの最初から2つの(仮想)ディレクトリが追加で表示されます(例:`www.example.com/en/products/`)。
- **URLの3レベル(3 levels of URL)**: レポートには、URLの最初から3つの(仮想)ディレクトリが追加で表示されます(例:`www.example.com/en/products/new/`)。

エグゼクティブレポートの設定(Executive Report Settings)

このエリアで、保持するエグゼクティブレポートの数をそれぞれ定義できます。

- デイリーレポート:最大60
- ウィークリーレポート:最大52
- マンスリー:最大12

設定を保存するには【*適用(Apply)*】をクリックします。

エグゼクティブレポートとそのオプションに関する詳細は、「*ログおよびレポーティング*」>>「*エグゼクティブレポート*」を参照してください。

PDF用紙設定(PDF Paper Settings)

PDFエグゼクティブレポートのデフォルトの用紙サイズはA4です。ドロップダウンリストを使用して、【*レター(Letter)*】または【*リーガル(Legal)*】を選択できます。設定を保存するには【*適用(Apply)*】をクリックします。

17.11.2除外

*【レポーティング設定(Reporting Settings)】>>【除外(Exceptions)】*タブで、特定のドメインやアドレスをレポートから除外できます。これはエグゼクティブレポートおよびそれぞれの*【レポーティング(Reporting)】*セクションに影響を及ぼします。以下のレポートに対して除外ルールを定義できます。

- Webセキュリティ(Web Security):ドメイン
- メールセキュリティ(Mail Security):ドメインおよびアドレス
- ネットワークセキュリティ(Network Security):IPアドレス

それぞれのボックスで除外項目を定義して*【適用(Apply)】*をクリックします。インポート機能によって複数の項目を一度に定義できます。

17.11.3匿名化

*【レポーティング設定(Reporting Settings)】>>【匿名化(Anonymizing)】*タブでは、「4つの目の原則」(four-eyes principle)に基づいてデータを匿名にできます。これは、2人の人間がその手順を承認した場合のみ非匿名化できることを意味します。匿名にすると、ユーザデータのログやレポートを表示する際にそのデータの機密性が保たれるため、アクション(Webサーフィンなど)から特定の人間にトレースバックする(さかのぼる)ことができなくなります。

図181 レポーティング:ユーザデータの匿名化の有効化

匿名にするには、以下の手順に従います。

1. ***【匿名化(Anonymizing)】*タブで匿名化を有効にします。**
   ステータスアイコンまたは*【有効(Enable)】*ボタンをクリックします。

ステータスアイコンがアンバー色に変わり【*匿名化設定(Anonymizing Setting)*】エリアが編集可能になります。

2. **2つのセキュリティパスワードを入力します。**
   「4つの目の原則」は、異なる2人の人間が互いが秘匿しているパスワードを入力したときのみ有効です。

3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

匿名化を再度グローバルに無効にするには、その両方のパスワードが必要になります。

1. **【*匿名化(Anonymizing)*】タブで【*無効(Disable)*】あるいはステータスアイコンをクリックします。**
   ステータスアイコンがアンバー色に変わり【*匿名化設定(Anonymizing Setting)*】エリアが編集可能になります。

2. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。

3. **【*適用(Apply)*】をクリックします。**
   設定が保存されます。

必要に応じて、匿名化を1人のユーザに対して無効にできます。詳細は「*ログおよびレポーティング*」>>「*Webセキュリティ*」および「*ログおよびレポーティング*」>>「*メールセキュリティ*」を参照してください。

１８サポート

この章では、当製品で使用できるサポートツールについて説明します。Astaro Security Gateway.

*【サポート(Support)】*メニューのページには、さまざまなWebリンク、お問い合わせ情報、役立つネットワークツールの出力など、お客様サポート関連の多数の機能が含まれています。これらを活用されることで、ゲートウェイのコマンドラインインタフェースを使用しないで、重要なネットワークプロパティを判断することができます。

この章には次のトピックが含まれます。

- マニュアル
- 印刷可能設定
- サポートのお問い合わせ先
- 【ツール(Tools)】
- 詳細

さらに、*【サポート(Support)】*メニューのメインページには、以下の情報へのWebリンクが含まれています。

- **ナレッジベース(Knowledgebase)**(KB):Astaroの公式ナレッジベースには、当製品の設定に関するさまざまな情報が掲載されています。Astaro Security Gateway.
- **既知の問題のリスト(Known Issues List)**(KIL):解決できない既知の問題や対応策のある既知の問題のリストです。
- **ハードウェア互換性リスト(Hardware Compatibility List)**(HCL):Astaro Security Gatewayソフトウェアに対応するハードウェアのリストです。
- **Up2Date情報(Up2Date Information)**: AstaroのUp2Dateブログには、製品の改善やファームウェアの更新についての情報が掲載されています。

１８.１マニュアル

【サポート(Support)】>>*【マニュアル(Manual)】*ページでは、現在の管理ガイドをPDF形式でダウンロードすることができます。ガイドの言語を選択し、*【ダウンロード(Download)】*をクリックします。PDF文書を開くためには、Adobe ReaderやXpdfといった特別なリーダーが必要です。

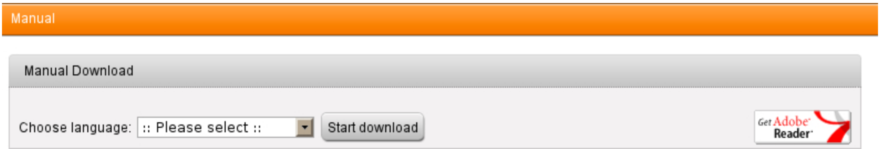


図182 サポート(Support):ダウンロード - 管理ガイド / Astaro Security Gateway

注 -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL (`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの【*インターネットオプション*】>>【*セキュリティ*】で設定します。さらに、Internet Explorer 7を使用する場合は、【*信頼済みサイトゾーン*】で【*ファイルのダウンロード時に自動的にダイアログを表示*】を選択します。

18.2印刷可能設定

【*サポート(Support)*】>>【*印刷可能設定(Printable Configuration)*】ページでは、現在のWebAdmin設定について詳細なレポートを作成できます。

注 - 印刷可能設定は新しいウィンドウで開きます。ブラウザによっては、WebAdmin用にポップアップウインドウを許可する必要があります。

印刷可能設定の構造は、WebAdminメニューの構造と同じであるため、対応するWebAdminの設定オプションを簡単に見つけることができます。

印刷可能設定ブラウザページは、概要ページ(*索引*)と複数のサブページから成ります。サブページへのリンクはブルーでハイライトされています。サブページには、関連トピックの詳細情報が表示されます。サブページの下部にある【*索引に戻る(Back to the index)*】リンクをクリックして、いつでもサブページから索引に戻ることができます。

印刷可能設定には他に2つの表示オプションがあります。

- WebAdmin形式
- Confd形式

これらの表示オプションへのリンクは、索引ページの下部にあります。

18.3サポートのお問い合わせ先

Astaroは、セキュリティソリューションのために総合的なお客様サポートサービスを提供しています。お客様のサポート/メンテナンスレベルに応じて、さまざまなレベルのアクセスサービスを提供し、認定パートナーにより様々なレベルのサポートが用意されています。

Astaro Security Gatewayに関連するすべてのサポートケースは、Astaroパートナーポータル経由で処理されます。サポートケースを開くには、*【サポートケースを開く(Open Support Case)】*をクリックしてWebフォームをご使用ください。

18.4ツール

【サポート(Support)】>>*【ツール(Tools)】*メニューのタブには、有用なネットワークツールの出力が表示されます。これらを使用すると、ゲートウェイのコマンドラインインタフェースを使用しないで、重要なネットワークプロパティを判断することができます。ここでは、以下のツールの出力を見ることができます。

- Ping
- Traceroute
- DNSルックアップ

18.4.1Pingチェック

*ping*プログラムは、IPネットワークを横断して特定ホストに到達できるかどうかをテストするためのコンピュータネットワークツールです。pingはICMP*エコー要求*パケットをターゲットホストに送信し、ICMP*エコー応答*による返信をリスンすることで機能します。pingは、間隔のタイミングと応答率を使用して、ホスト間の往復時間とパケット紛失率を評価します。

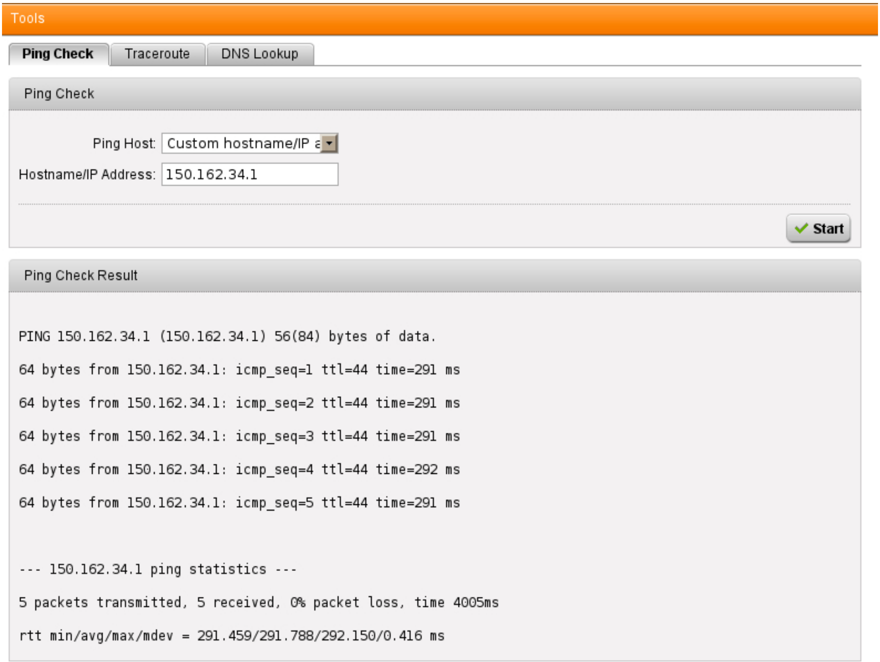


図183 サポート(Support):pingを使用したホストの可用性チェック

pingチェックを行うには、以下の手順に従います。

1. **pingホストを選択します。**
   pingするホストを選択します。【*Pingホスト(Ping Host)*】ボックスで、ホスト定義のあるホストを選択できます。または、【*カスタムホスト名/IPアドレス(Custom hostname/IP address)*】を選択してカスタムホスト名またはIPアドレスを下のテキストボックスに入力することもできます。

2. ***【開始(Start)】をクリックします。***
   pingチェックの出力が【*Pingチェック結果(Ping Check Result)*】エリアに表示されます。

18.4.2Traceroute

traceroute(トレースルート)プログラムは、IPネットワーク上でパケットが使用するルートの決定に使用されるコンピュータネットワークツールです。tracerouteは、パケットの伝送に関与したルータのIPアドレスを一覧表示します。一定の時間内にパケットのルートを判断できない場合は、IPアドレスの代わりにアスタリスク(*)で報告します。一定の回数だけ失敗すると、確認作業は終了し

ます。確認の中断には多くの理由が考えられますが、ほとんどの場合は、ネットワークパスのファイアウォールがtracerouteパケットをブロックすることが原因となります。

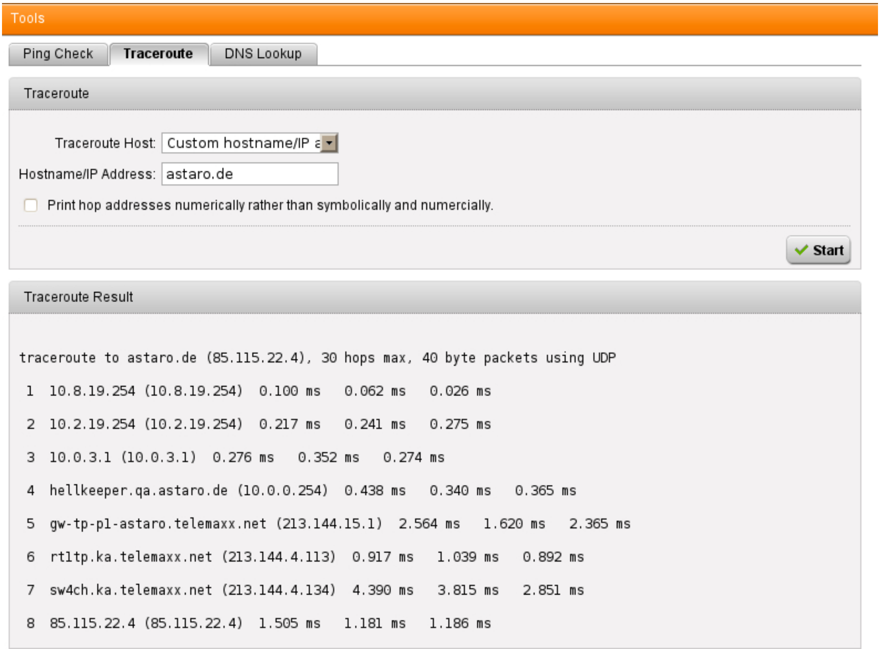


図184 サポート(Support):tracerouteを使用したルートの確認

ルートを追跡するには、以下の手順に従います。

1. **ホスト名/IPアドレスを指定します。**
   ルートを判断したいホストのホスト名またはIPアドレスを入力します。

2. **ホップアドレスを数値で出力します**(オプション)。
   パスで見つかった各ゲートウェイについて、ネームサーバでIPアドレスからDNSホスト名への名前解決を行わない場合は、このオプションを選択します。

3. ***【開始(Start)】*をクリックします。**
   tracerouteの出力が**【*トレースルートの結果(Traceroute Result)*】**エリアに表示されます。

18.4.3DNSルックアップ

*dig*プログラム(*Domain Information Groper*の略)は、DNSネームサーバに問い合わせを行うネットワークツールです。digプログラムはDNSルックアップを実行し、クエリしたネームサーバから返された応答を表示します。

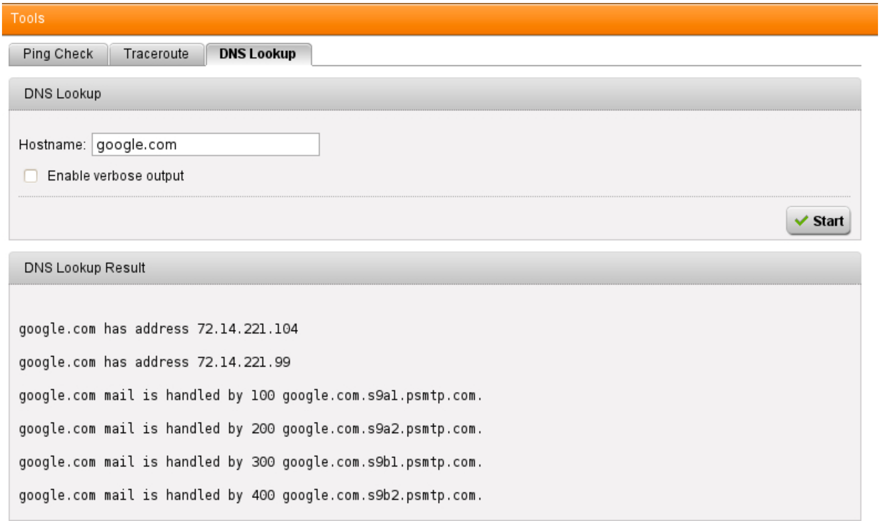


図185 サポート(Support):digを使用したDNSエントリのルックアップ

DNSルックアップを行うには、以下の手順に従います。

1. **ホスト名/IPアドレスを指定します。**
   DNS情報を判定したいホストのホスト名またはIPアドレスを入力します。
2. ***【詳細な出力を有効にする(Enable Verbose Output)】***を選択します(オプション)。
   このオプションを選択すると、より詳細な情報が出力されます。
3. ***【開始(Start)】*をクリックします。**
   digの出力が*【DNSルックアップの結果(DNS Lookup Result)】*エリアに表示されます。

18.5詳細

*【サポート(Support)】>>【詳細(Advanced)】*メニューには、ゲートウェイに関するより詳細な情報(プロセスの状態など)が表示されます。

18.5.1プロセスリスト

*ps*プログラムは、ヘッダ行に続き、コントロール端末を持つプロセスに関する情報を表示します。この情報は、コントロール端末毎にソートされ、次にプロセスID毎にソートされます。

18.5.2ローカルネットワークコネクション

プログラム*netstat*(「*ネットワーク統計*」の略語)とは、コンピュータに現在存在するアクティブなインターネット接続(受信と送信の両方)のリストを表示するネットワークツールです。

18.5.3ルーティングテーブル

*ip*プログラムは、TCP/IPネットワークのコントロールとトラフィックコントロールのためのネットワークツールです。パラメータ`route show table all`で起動されるこのプログラムは、ゲートウェイのすべてのルーティングテーブルの内容を表示します。

18.5.4インタフェーステーブル

このテーブルには、Astaro Security Gatewayのすべての設定済みインタフェース(ネットワークインタフェースカードと仮想インタフェースの両方)が表示されます。`addr`パラメータで起動した*ip*プログラムが、インタフェースとそのプロパティを表示します。

18.5.5コンフィグダンプ

デバッグやリカバリのために、Astaro Security Gatewayのインストールに関してできるだけ多くの情報を収集しておくと便利です。*【サポート(Support)】*>>*【詳細(Advanced)】*>>*【コンフィグダンプ(Config Dump)】*タブでダウンロードできるサポートパッケージは、これに対応します。`zip`ファイルには次のアイテムが含まれています。

- ゲートウェイの設定の全ダンプ(`storage.abf`)。これは真のバックアップファイルではないため、パスワードなどが含まれておらず、デバッグ目的のみで使用できます。
- システム内に存在するハードウェアに関する情報(`hwinfo`)。
- システムにインストールされたソフトウェアパッケージに関する情報(`swinfo`)。

注 -Internet Explorer(IE)6を使用したファイルのダウンロードで問題が起こらないようにするには、ゲートウェイのURL(`https://192.168.2.100`など)を信頼されるサイトに追加します。これはIEの*【インターネットオプション】*>>*【セキュリティ】*で設定します。さらに、Internet Explorer 7を使用する場合は、*【信頼済みサイトゾーン】*で*【ファイルのダウンロード時に自動的にダイアログを表示】*を選択します。

18.5.6REFの解決

デバッグのために、システム内部で使用されている設定リファレンスを解決することができます。ログ内でリファレンスを見つけた場合、リファレンス文字列をここに貼り付けてください(例:`REF_DefaultSuperAdmin`)。タブに、設定用Configurationデーモンのデータ構造の該当箇所が表示されます。

１９ログオフ

WebAdminからログアウトするには、【*ログオフ(Log Off)*】メニューエントリをクリックします。適切にログアウトしなかった場合や、Webブラウザを誤って閉じてしまった場合には、約30秒間再ログインできない可能性があります。

注 - セッション中に別のWebサイトにアクセスした場合にも、ログアウトしたことになります。この場合、ログインしなおす必要があります。

用語集

3

3DES

Triple Data Encryption Standard(トリプルデータ暗号化標準)

A

ACPI

Advanced Configuration and Power Interface(アドバンスドコンフィギュレーションアンドパワーインタフェース)

AD

Active Directory

ADSL

Asymmetric Digital Subscriber Line(非対称デジタル加入者線)

AES

Advanced Encryption Standard(高度暗号化標準)

AFC

Astaro Flow Classifier

AH

Authentication Header(認証ヘッダ)

AMG

Astaro Mail Gateway

APIC

Advanced Programmable Interrupt Controller(アドバンスドプログラマブルインタラプトコントローラ)

ARP

Address Resolution Protocol(アドレス解決プロトコル)

AS

Autonomous System(自律システム)

ASCII

American Standard Code for Information Interchange(情報交換用米国標準コード)

ASG

Astaro Security Gateway

ASG:WebAdmin-ネットワークサービス-DHCP

Dynamic Host Configuration Protocol(ダイナミックホスト設定プロトコル)

ASG:WebAdmin-ネットワークサービス-DNS

Domain Name Service(ドメインネームサービス)

ASG:WebAdmin-ネットワークサービス-NTP

Network Time Protocol(ネットワークタイムプロトコル)

ASG:WebAdmin-マネジメント-SNMP

Simple Network Message Protocol(シンプルネットワークメッセージプロトコル)

ASG:WebAdmin-メールセキュリティ-POP3

Post Office Protocol version 3(ポストオフィスプロトコルバージョン3)

ASG:WebAdmin-メールセキュリティ-SMTP

Simple Mail Transfer Protocol(簡易メール転送プロトコル)

Astaro Security Gateway

メールとWebセキュリティを含む、統合脅威管理のためのソフトウェア。

AUA

Astaro User Authentication

AWG

Astaro Web Gateway

B

BATV

Bounce Address Tag Validation(バウンスアドレスタグ検証)

C

CA

Certificate Authority(認証局)

CBC

Cipher Block Chaining(暗号ブロック連鎖)

CHAP

Challenge-Handshake Authentication Protocol(チャレンジハンドシェイク認証プロトコル)

CMS

Content Management System(コンテンツ管理システム)

CRL

Certificate Revocation List(証明書失効リスト)

CSS

Cascading Style Sheets(カスケーディングスタイルシート)

D

DC

Domain Controller(ドメインコントローラ)

DCC

Direct Client Connection(直接クライアント接続)

DDoS

Distributed Denial of Service(分散型サービス拒否)

DER

Distinguished Encoding Rules(識別符号化規則)

DKIM

Domain Keys Identified Mail(ドメインキー識別メール)

DMZ

Demilitarized Zone

DN

Distinguished Name(識別名)

DNAT

Destination Network Address Translation(宛先ネットワークアドレス変換)

DOI

Domain of Interpretation(解釈ドメイン)

DoS

Denial of Service(サービス拒否)

DSA

Digital Signature Algorithm(デジタル署名アルゴリズム)

DSCP

Differentiated Services Code Point(差別化サービスコードポイント)

DSL

Digital Subscriber Line(デジタル加入者線)

DUID

DHCP Unique Identifier(DHCP固有識別子)

E

ESP

Encapsulating Security Payload(カプセル化セキュリティペイロード)

F

FAT

File Allocation Table(ファイルアロケーションテーブル)

FQHN

Fully Qualified HostName(完全修飾ホスト名)

FTP

File Transfer Protocol(ファイル転送プロトコル)

G

GeoIP

衛星画像を使用して世界中のデバイスの位置を特定する技術。

GRE

Generic Routing Encapsulation(ジェネリックルーティングカプセル化)

H

H.323

パケット交換網上での音声・映像通信セッションを提供するプロトコル。

HA

High Availability(高可用性)

HCL

Hardware Compatibility List(ハードウェア互換性リスト)

HELO

SMTP(Simple Mail Transfer Protocol:簡易メール転送プロトコル)のコマンドであり、クライアントはサーバからの初期グリーティングに応答します。

HMAC

Hash-based Message Authentication Code(ハッシュベースのメッセージ認証コード)

HTML

Hypertext Transfer Markup Language(ハイパーテキスト転送マークアップ言語)

HTTP

Hypertext Transfer Protocol(ハイパーテキスト転送プロトコル)

HTTP over SSL

よりセキュアなHTTP通信を実現するプロトコル。

HTTP/S

Hypertext Transfer Protocol Secure(ハイパーテキスト転送プロトコルセキュア)

HTTPS

Hypertext Transfer Protocol Secure(ハイパーテキスト転送プロトコルセキュア)

I

IANA

Internet Assigned Numbers Authority(インターネット番号割当当局)

ICMP

Internet Control Message Protocol(インターネット制御メッセージプロトコル)

ID

Identity(アイデンティティ)

IDE

Intelligent Drive Electronics(インテリジェントドライブエレクトロニクス)

IDENT

特定のTCP接続のユーザを特定するための標準プロトコル。

IE

Internet Explorer

IE7

Internet Explorerバージョン7

IKE

Internet Key Exchange(インターネット鍵交換)

IM

Instant Messaging(インスタントメッセージ)

IP

Internet Protocol(インターネットプロトコル)

IPS

Intrusion Prevention System(侵入防止システム)

IPsec

Internet Protocol Security(インターネットプロトコルセキュリティ)

IPアドレス

インターネットプロトコル標準を使用するコンピュータネットワーク上の各デバイスが互いを特定し、通信するために使用する一意の番号。

IRC

Internet Relay Chat(インターネットリレーチャット)

ISP

Internet Service Provider(インターネットサービスプロバイダ)

L

L2TP

Layer Two (2) Tunneling Protocol(レイヤ2トンネリングプロトコル)

LAG

Link Aggregation Group(リンクアグリゲーショングループ)

LAN

Local Area Network(ローカルエリアネットワーク)

LDAP

Lightweight Directory Access Protocol(ライトウェイトディレクトリアクセスプロトコル)

LSA

Link-state advertisement(リンクステートアドバタイズメント)

M

MAC

Media Access Control(メディアアクセスコントロール)

MACアドレス

ほとんどの形態のネットワークハードウェアに割り当てられる一意のコード。

MD5

Message-Digest algorithm 5(メッセージダイジェストアルゴリズム5)

MIB

Management Information Base(管理情報ベース)

MIME

Multipurpose Internet Mail Extensions(多目的インターネットメール拡張)

MPPE

Microsoft Point-to-Point Encryption(マイクロソフトポイントツーポイント暗号化)

MSCHAP

Microsoft Challenge Handshake Authentication Protocol(マイクロソフトチャレンジハンドシェイク認証プロトコル)

MSCHAPv2

Microsoft Challenge Handshake Authentication Protocol Version 2(マイクロソフトチャレンジハンドシェイク認証プロトコルバージョン2)

MSSP

マネージドセキュリティサービスプロバイダ

MTU

Maximum Tansmission Unit(最大伝送単位)

MXレコード

インターネットでEメールをどのようにルーティングするのかを指定する、ドメインネームシステム(DNS)内のリソースレコードの種類。

N

NAS

Networked Attached Storage(ネットワークアタッチドストレージ)

NAT

Network Address Translation(ネットワークアドレス変換)

NAT-T

NAT Traversal(NATトラバーサル)

NIC

Network Interface Card(ネットワークインタフェースカード)

Not-so-stubbyエリア

OSPFプロトコルの中で、自律システム(AS)外部ルートをインポートし、それらをバックボーンに送信することはできるが、バックボーンやその他のエリアからAS外部ルートを受信することはできないタイプのスタブエリア。

NSSA

Not-so-stubby area(Not-so-stubbyエリア)

NTLM

NT LAN Manager(Microsoft Windows)

O

OpenPGP

強力な公開鍵と対称暗号を組み合わせて、電子通信とデータストレージのためのセキュリティサービスを提供するプロトコル。

OSI

Open Source Initiative(オープンソースイニシアチブ)

OSPF

Open Shortest Path First(オープンショーテストパスファースト)

OU

Organisational Unit(組織単位)

P

PAC

Proxy Auto Configuration(プロキシの自動設定)

PAP

Password Authentication Protocol(パスワード認証プロトコル)

PCI

Peripheral Component Interconnect(ペリフェラルコンポーネントインターコネクト)

PEM

Privacy Enhanced Mail(プライバシ拡張メール)

PGP

Pretty Good Privacy(プリティグッドプライバシ)

PKCS

Public Key Cryptography Standards(公開鍵暗号標準)

PKI

Public Key Infrastructure(公開鍵暗号基盤)

PMTU

Path Maximum Transmission Unit(パス最大伝送単位)

Post Office Protocol version 3(ポストオフィスプロトコルバージョン3)

パケット交換網上でEメールを配信するためのプロトコル。

PPP

Point-to-Point Protocol(ポイントツーポイントプロトコル)

PPPoA

PPP over ATM Protocol(PPPオーバーATMプロトコル)

PPTP

Point to Point Tunneling Protocol(ポイントツーポイントトンネリングプロトコル)

PSK

事前共有鍵(Preshared Key)

Q

QoS

Quality of Service(サービス品質)

R

RADIUS

Remote Authentication Dial In User Service(リモート認証ダイヤルインユーザサービス)

RAID

Redundant Array of Independent Disks(独立ディスク冗長アレイ)

RAM

Random Access Memory(ランダムアクセスメモリ)

RAS

Remote Access Server(リモートアクセスサーバ)

RBL

Realtime Blackhole List(リアルタイムブラックホールリスト)

RDN

Relative Distinguished Name(相対識別名)

RDNS

Reverse Domain Name Service(リバースドメインネームサービス)

RED

Random Early Detection(ランダム初期検知)

Redundant Array of Independent Disks(独立ディスク冗長アレイ)

複数のハードドライブを使用してドライバ間でデータを共有または複製するデータ保管スキーム。

RFC

Request for Comment(リクエストフォーコメント)

RPS

RED Provisioning Service

RSA

Rivest, Shamir, & Adleman(リベスト、シャミア、エーデルマン:公開鍵暗号化技術)

S

S/MIME

Secure/Multipurpose Internet Mail Extensions(セキュア多目的インターネットメール拡張)

SA

Security Associations(セキュリティアソシエーション)

SCP

Secure Copy(セキュアコピー: セキュア通信用のSSHコンピュータアプリケーションスイートからの)

SCSI

Small Computer System Interface(スモールコンピュータシステムインタフェース)

Session Initiation Protocol(セッション開始プロトコル)

2つ以上の通信パートナー間でセッションを確立、変更、終了するためのシグナリングプロトコル。このテキスト指向のプロトコルはHTTPをベースとしており、IPネットワーク経由でTCPまたはUDPを通して信号データを送信できる。そのため、VoIP(Voice-over-IP)ビデオ電話やリアルタイムなマスチメディアサービスなどの基盤となる。

SFQ

Stochastic Fairness Queuing(確率的不偏キューイング)

SIP

Session Initiation Protocol(セッション開始プロトコル)

SMB

Server Message Block(サーバメッセージブロック)

SMP

Symmetric Multiprocessing(対称型マルチプロセッシング)

SNAT

Source Network Address Translation(送信元ネットワークアドレス変換)

SOCKetS

クライアントサーバアプリケーションがネットワークファイアウォールのサービスを透過的に使用できるようにするインターネットプロトコル。現在、SOCKS(別名:ファイアウォールトラバースプロトコル)はバージョン5であり、正しく機能するためにはクライアント側のプログラムに導入する必要がある。

SOCKS

SOCKetS

SPF

Sender Policy Framework(送信者ポリシフレームワーク)

SPI

Security Parameter Index(セキュリティパラメータインデックス)

SSH

Secure Shell(セキュアシェル)

SSID

Service Set Identifier(サービスセット識別子)

SSL

Secure Sockets Layer(セキュアソケットレイヤ)

SSO

Single sign-on(シングルサインオン)

SYN

Synchronous(同期)

T

TACACS

Terminal Access Controller Access Control System(ターミナルアクセスコントローラアクセスコントロールシステム)

TCP

Transmission Control Protocol(伝送制御プロトコル)

TFTP

Trivial File Transfer Protocol(簡易ファイル転送プロトコル)

TKIP

Temporal Key Integrity Protocol(一時鍵完全性プロトコル)

TLS

Transport Layer Security(トランスポートレイヤセキュリティ)

TOS

Type of Service(サービスタイプ)

TTL

Time-to-live(生存時間)

U

UDP

User Datagram Protocol(ユーザデータグラムプロトコル)

Up2Date

Astaroサーバから関連する更新パッケージをダウンロードするためのサービス。

UPS

Uninterruptible Power Supply(無停電電源装置)

URL

Uniform Resource Locator(ユニフォームリソースロケータ)

USB

Universal Serial Bus(ユニバーサルシリアルバス)

UTC

Coordinated Universal Time(協定世界時)

V

VDSL

Very High Speed Digital Subscriber Line(超高速デジタル加入者線)

VLAN

Virtual LAN(バーチャルLAN)

VoIP

Voice over IP(ボイスオーバーIP)

VPN

Virtual Private Network(バーチャルプライベートネットワーク)

W

WAF

Web Application Firewall(Webアプリケーションファイアウォール)

WAN

Wide Area Network(ワイドエリアネットワーク)

WebAdmin

ACC、ASG、AWG、およびAMGといったAstaro製品のためのWebベースGUI。

WEP

Wired Equivalent Privacy(有線同等機密)

Windowsインターネットネーミングサービス

マイクロソフトがWindowsに実装したNBNS(NetBIOS Name Server:NetBIOSネームサーバ)。NetBIOSコンピュータ名のためのネームサーバおよびサービスである。

WINS

Windows Internet Naming Service(Windowsインターネットネーミングサービス)

WPA

Wi-Fi Protected Access(Wi-Fi保護アクセス)

X

X.509

ITU-T(国際電気通信連合、電気通信標準化部門)が公開したデジタル証明書の仕様。個人またはコンピュータシステムの識別に必要な情報や属性を規定する。

XSS

Cross-site scripting(クロスサイトスクリプティング)

ア

アドバンスドコンフィグレーションアンドパワーインタフェース

ACPIとは電力管理標準の1つであり、コンピュータ内の各デバイスに分散させる電力量をオペレーティングシステムで制御できるようにするものです。

アドバンスドプログラマブルインタラプトコントローラ

マルチプロセッサコンピュータシステムでの割り込みを処理するアーキテクチャ。

アドレス解決プロトコル

ホストのIPアドレスしかわからない場合に、そのイーサネットMACアドレスを確定するために使用される。

イ

インターネットサービスプロバイダ

インターネットや関連サービスへのアクセスを利用者に販売する企業または組織。

インターネットプロトコル

パケット交換網上でのデータ通信に使用されるデータ指向プロトコル。

インターネットリレーチャット

インターネット上でのインスタント通信を可能にするオープンプロトコル。

インターネット制御メッセージプロトコル

ネットワークのステータスやその他のコントロール情報についての情報を送受信するために使用される特別なIPプロトコル。

オ

オープンショーテストパスファースト

ネットワークルーティングのための、リンクステート型の階層的なIGP(interior gateway protocol)。

カ

カプセル化セキュリティペイロード

データの機密性(暗号)、アンチリプレイ、認証を提供するIPSecプロトコル。

ク

クラスタ

リンクされたコンピュータのグループ。緊密に連携して多くの局面で1台のコンピュータとして機能する。

サ

サブネットマスク

ネットワークのサブネットマスク(別名:ネットマスク)とネットワークアドレスによって、ローカルネットワークの一部となるアドレスとならないアドレスが定義される。個々のコンピュータは、この定義に基づいてネットワークに割り当てられる。

ジ

ジェネリックルーティングカプセル化

任意のネットワーク層パケット内で任意のネットワーク層パケットをカプセル化するために規定されたトンネリングプロトコル。

シ

シングルサインオン

ユーザが一度だけ認証を行い、1つのパスワードを使用して複数のアプリケーションやシステムにアクセスできるようにする認証方式。

セ

セキュアシェル

異なるパケット交換網にまたがるローカルコンピュータとリモートコンピュータの間でセキュアなチャネルを確立するためのプロトコル。

セキュアソケットレイヤ

インターネット上でセキュアな通信を提供する暗号プロトコル。TLS(トランスポートレイヤセキュリティ)の前身である。

セキュア多目的インターネットメール拡張

MIMEにカプセル化されたEメールに対する公開鍵暗号化や署名のための標準。

セキュリティパラメータインデックス

IPトラフィックのトンネリングにIPSecを使用するときにヘッダに追加される識別タグ。

ソ

ソフトウェアが次のハードウェアコンポーネントをチェックします。

Central Processing Unit(中央処理装置)

ダ

ダイナミックホスト設定プロトコル

ネットワーク上のデバイスがIPアドレスを取得するために使用するプロトコル。

デ

デジタル加入者線

地域電話網のケーブル上でのデジタルデータ伝送を提供する技術群。

デジタル署名アルゴリズム

米国連邦政府が推奨しているデジタル署名についての標準(FIPS)。

デバイスツリー

メインメニューの下にあり、ACCに登録されたすべてのAstaroゲートウェイ装置にアクセス権を付与する。

ド

ドメインネームサービス

インターネットを介して接続されたコンピュータの基底のIPアドレスを、人にとってわかりやすい名前やエイリアスに変換する。

ト

トランスポートレイヤセキュリティ

インターネット上でセキュアな通信を提供する暗号プロトコル。SSL(セキュアソケットレイヤ)の後継プロトコルである。

ネ

ネットワークアドレス変換

IPアドレスを再利用するためのシステム。

ネットワークタイムプロトコル

パケット交換網上でコンピュータシステムのクロックを同期するためのプロトコル。

バ

バーチャルプライベートネットワーク

公衆通信インフラを利用するプライベートデータネットワーク。PPTPやIPSecなどのトンネリングプロトコルを使用してプライバシを維持する。

ハ

ハイパーテキスト転送プロトコル

インターネット上で情報を転送するためのプロトコル。

バウンスアドレスタグ検証

Eメールメッセージに指定された返信アドレスが有効であるかどうかを判定するために規定された手法の名前。偽造された返信アドレスへのバウンスメッセージを拒否するように設計されている。

フ

ファイル転送プロトコル

パケット交換網上でのファイル交換用プロトコル。

プ

プライバシ拡張メール

公開鍵暗号を使用してEメールのセキュリティを保護するための、初期のIETF提案。

ブ

ブロードキャスト

ネットワーク内の他のすべてのコンピュータに向けてメッセージを一括送信するためにコンピュータで使用されるアドレス。たとえば、IPアドレスが192.168.2.0でネットワークマスクが255.255.255.0のネットワークは、ブロードキャストアドレスが192.168.2.255となる。

プロキシ

クライアントが他のネットワークサービスに対して間接的にネットワーク接続できるようにするコンピュータネットワークサービスを提供するコンピュータ。

プロトコル

2つのコンピュータエンドポイント間での接続、通信、データ転送を制御または実現するための、明確で標準化されたルールセット。

ボ

ボイスオーバーIP

インターネット上またはその他のIPベースのネットワーク上での音声会話ルーティング。

ポ

ポート

データを直接交換するためにプログラムで使用できる仮想データ接続。具体的には、ポートとは追加の識別子である(TCPとUDPの場合、0～65535の番号)。これにより、コンピュータはある2台のコンピュータ間に存在する複数の同時接続を見分けることができる。

ポートスキャン

ネットワークホストの空きポートを探す行為。

マ

マスカレーディング

LAN全体で1つのパブリックIPアドレスを使用してインターネットの他の部分と通信できるようにするNATベースの技術。

マネージドセキュリティサービスプロバイダ

企業に対してセキュリティサービスを提供する。

メ

メッセージダイジェストアルゴリズム5

128ビットのハッシュ値による暗号ハッシュ関数。

ユ

ユーザデータグラムプロトコル

ネットワーク上のコンピュータのアプリケーションで短いメッセージ(別名:データグラム)をやりとりするためのプロトコル。

ユニフォームリソースロケータ

インターネット上のリソースの位置を指定する文字列。

リ

リアルタイムブラックホールリスト

スパム行為に関与しているIPアドレスのリストをインターネットサイトが公開できる手段。ほとんどのメール転送エージェント(メールサーバ)ソフトウェアは、1つ以上のブラックホールリストに記載されたサイトから送信されたメッセージを拒否したりフラグを付加したりするように設定できる。

リモート認証ダイヤルインユーザサービス

ルータなどのネットワークデバイスが中央データベースに対してユーザを認証できるように設計されたプロトコル。

リンクステートアドバタイズメント

IP用のOSPFルーティングプロトコルの基本的な通信手段。

ル

ルータ

最も効率の良いパスで宛先までパケットを転送するために指定されるネットワークデバイス。

宛

宛先ネットワークアドレス変換

データパケットの宛先アドレスを書き換える特殊なNAT。

暗

暗号ブロック連鎖

暗号処理モードの1つであり、平文(プレーンテキスト)の各ブロックを直前の暗号文ブロックと「排他的論理和(XOR)」してから暗号化する。これにより、暗号文の各ブロックはその時点までのすべての平文ブロックに依存するようになる。

管

管理情報ベース

通信ネットワーク内のデバイスを管理するために使用されるデータベースの種類。ネットワーク内のエンティティ(ルータやスイッチなど)を管理するために使用される(仮想)データベース内のオブジェクトの集合から構成される。

簡

簡易メール転送プロトコル

パケット交換網上でEメールを送受信するために使用されるプロトコル。

関

関連トピック

複数のAstaroゲートウェイ装置を1つのインタフェースで監視・管理するためのソフトウェア。

共

共有シークレット

セキュア通信の2つのエンティティ間で共有されているパスワードまたはパスフレーズ。

高

高可用性

信頼できるレベルの運用継続性を確実に保証するためのシステム設計プロトコル。

自

自律システム

1つのエンティティによって管理されるIPネットワークとルータの集合体であり、インターネットに対して共通のルーティングポリシを持つ。

識

識別符号化規則

X.509証明書などデジタル署名または署名が検証されるデータオブジェクトを符号化するための方式。

生

生存時間

IP(インターネットプロトコル)ヘッダ内の8ビットのフィールドであり、パケットをネットワーク経由で伝送できる制限時間を指定する。この時間が経過すると、そのパケットは廃棄される。

送

送信元ネットワークアドレス変換

特殊なNAT。SNATでは、接続を開始したコンピュータのIPアドレスが書き換えられる。

送信者ポリシフレームワーク

SMTP(Simple Mail Transfer Protocol:簡易メール転送プロトコル)の拡張。SPFを使用すると、スパムによく見られるSMTP MAIL FROM(リターンパス)の偽造アドレスをソフトウェアで特定し、拒否することができる。

多

多目的インターネットメール拡張

Eメールのフォーマットを拡張し、US-ASCII以外の文字セットのテキスト、テキスト以外の添付物、マルチパートメッセージ本体、ASCII以外の文字セットでのヘッダ情報をサポートするためのインターネット標準。

対

対称型マルチプロセッシング

複数CPUを使用すること。

伝

伝送制御プロトコル

インターネットプロトコルスイートのプロトコル。これにより、ネットワーク内のコンピュータ上のアプリケーションが相互接続できる。このプロトコルによって、データが送信者から受信者へ確実かつ順序通りに送信される。

認

認証ヘッダ

アンチリプレイを提供し、伝送中にパケットの内容が改ざんされていないことを検証するIPSecプロトコル。

認証局

他のパーティによって使用されるデジタル証明書を発行する団体または組織。

無

無停電電源装置

接続された機器に対する継続的な配電を維持するためのデバイス。通常電源を使用できないときには別の電源から電力を供給する。

図 のリスト

図1 IE7 セキュリティ設定信頼済みサイト ゾーン..15
図2 WebAdmin:初期ログインページ..22
図3 WebAdmin:通常のログインページ..23
図4 WebAdmin:ダッシュボード..26
図5 WebAdmin:概要..29
図6 WebAdmin:リストの例..32
図7 WebAdmin:ダイアログボックスの例..33
図8 WebAdmin:オブジェクトリストネットワークからのオブジェクトのドラッグ................35
図9 WebAdmin:ASGソフトウェアのサンプルダッシュボード V8..37
図10 システム設定:日付および時間を設定..47
図11 WebAdmin設定:アクセスコントロールの設定..51
図12 WebAdmin設定:ユーザ設定の内容..55
図13 MyAstaroポータル..58
図14 ライセンス(Licensing):サブスクリプション警告メッセージ..63
図15 ライセンス(Licensing):概要(オンデマンドライセンス)(Overview(OnDemand Licensing))..64
図16 ライセンス(Licensing):ライセンスのインストール..65
図17 Up2Date:【概要(Overview)】ページ..67
図18 Up2Date:進捗ウィンドウ..68
図19 Up2Date:Up2Dateパッケージの暗黙的インストール..69
図20 ユーザポータル:「ようこそ」のページ..76
図21 ユーザポータル:ユーザポータルへのアクセスの設定..78
図22 カスタマイズ:ブロックされるページの例とカスタマイズ可能な部分..82
図23 カスタマイズ:HTTPダウンロードページ、ステップ1/3..85
図24 カスタマイズ:HTTPダウンロードページ、ステップ2/3..85
図25 カスタマイズ:HTTPダウンロードページ、ステップ3/3..86
図26 カスタマイズ:POP3プロキシのブロックメッセージ..86
図27 SNMP:SNMPクエリの設定..88
図28 集中管理:Astaro Command Centerのダッシュボード..92
図29 集中管理:ACC V2サーバの使用..93
図30 冗長化(HA):【ステータス(Status)】ページ..96
図31 冗長化:シングルHAまたはクラスタデバイスのリソース使用状況..98
図32 冗長化:クラスタの設定..100

図33 定義(Definitions):ネットワーク定義のリスト 106
図34 定義(Definitions):サービス定義リスト 109
図35 定義(Definitions):タイムイベント定義リスト 112
図36 ユーザ(Users):ユーザリスト 114
図37 グループ:グループのリスト 116
図38 グループ(Groups):eDirectoryブラウザ - Astaro Security Gateway 119
図39 認証(Authentication):eDirectoryの設定 123
図40 認証(Authentication):Active Directoryユーザ認証の設定 125
図41 認証(Authentication):Microsoft Management Console 127
図42 認証(Authentication):LDAPの設定 128
図43 認証(Authentication):RADIUSの設定 131
図44 認証(Authentication):TACACS+ユーザ認証の設定 133
図45 認証(Authentication):シングルサインオンの設定 135
図46 インタフェース(Interfaces):インタフェースの設定 141
図47 インタフェース(Interfaces):アップリンクバランシングの設定 160
図48 インタフェース(Interfaces):マルチパスルール 163
図49 ブリッジ:ブリッジの設定 166
図50 ブリッジ:ブリッジングが有効 167
図51 ブリッジ:ブリッジを無効にする 168
図52 スタティックルーティング:スタティックルートテーブル 169
図53 スタティックルーティング:ポリシルートテーブル 171
図54 OSPF:OSPFの有効化 173
図55 OSPF:設定されたエリアの概要 174
図56 QoS:【ステータス(Status)】ページ 185
図57 QoS:トラフィックセレクタ 187
図58 QoS:帯域幅プール 191
図59 PIM-SM:設定例 193
図60 PIM-SM:インタフェースリスト 194
図61 PIM-SM:ランデブーポイントルータのリスト 196
図62 PIM-SM:ルートリスト 197
図63 DNS:DynDNSの設定 204
図64 DHCP:DHCPリレーの設定 209
図65 DHCP:IPv4リーステーブル 211
図66 DHCP:IPv6リーステーブル 212
図67 ファイアウォール(Firewall):ルールテーブル 216
図68 ファイアウォール(Firewall):ライブログ 218

図69 NAT:マスカレードルールのリスト ... 224
図70 NAT:DNAT/SNATルールのリスト ... 226
図71 IPS:侵入防御を有効にする ... 229
図72 IPS:攻撃パターン ... 231
図73 IPS:ポートスキャン防御の設定 ... 234
図74 IPS:除外リスト ... 236
図75 サーバロードバランシング:負荷分散ルールリスト ... 239
図76 VoIP SIP:VoIP SIPの有効化 ... 243
図77 VoIP H.323:VoIP H.323の有効化 ... 244
図78 ジェネリックプロキシ:ルールリスト ... 246
図79 Webフィルタ(Web Filter):グローバル設定 ... 250
図80 Webフィルタ(Web Filter):アンチウイルス/マルウェア設定の構成 ... 254
図81 Webフィルタ(Web Filter):URLフィルタリングの設定 ... 257
図82 Webフィルタ(Web Filter):除外リスト ... 262
図83 Webフィルタプロファイル:プロファイルのリスト ... 275
図84 Webフィルタプロファイル:フィルタ割り当てのリスト ... 279
図85 Webフィルタプロファイル:フィルタアクションのリスト ... 281
図86 FTPプロキシ(FTP Proxy):FTPプロキシを有効にする ... 290
図87 FTPプロキシ(FTP Proxy):アンチウイルス設定の構成 ... 292
図88 FTPプロキシ(FTP Proxy):除外リスト ... 293
図89 FTPプロキシ(FTP Proxy):詳細設定 ... 295
図90 SMTPプロキシ(SMTP Proxy):SMTPプロキシの有効化 ... 298
図91 SMTPプロキシ(SMTP Proxy):ドメインとルーティングターゲットの設定 ... 299
図92 SMTPプロキシ(SMTP Proxy):アンチウイルス設定の構成 ... 301
図93 SMTPプロキシ(SMTP Proxy):ファイル拡張子フィルタ(File Extension Filter) ... 303
図94 SMTPプロキシ(SMTP Proxy):アンチウイルスチェックフッタ ... 305
図95 SMTPプロキシ(SMTP Proxy):アンチスパム設定の構成 ... 306
図96 SMTPプロキシ(SMTP Proxy):送信者ブラックリストを拡張する ... 309
図97 SMTPプロキシ(SMTP Proxy):表現フィルタに表現を追加する ... 309
図98 SMTPプロキシ(SMTP Proxy):高度なアンチウイルス機能 ... 311
図99 SMTPプロキシ(SMTP Proxy):除外リスト ... 312
図100 SMTPプロキシ(SMTP Proxy):リレーの設定 ... 314
図101 SMTPプロキシ(SMTP Proxy):ホスト/ネットワークのブラックリストの有効化 ... 315
図102 SMTPプロキシ(SMTP Proxy):リレーメッセージのコンテンツスキャンの有効化 ... 316
図103 SMTPプロファイル:SMTPプロファイルの設定 ... 320
図104 POP3プロキシ(POP3 Proxy):POP3プロキシを有効にする ... 326

図105 POP3プロキシ(POP3 Proxy):アンチウイルス設定の構成 327
図106 POP3プロキシ(POP3 Proxy):アンチスパム設定の構成 329
図107 POP3プロキシ(POP3 Proxy):除外リスト 331
図108 POP3プロキシ(POP3 Proxy):詳細設定 333
図109 メール暗号化(E-mail Encryption):2つのAstaro Security Gateway ユニットの使用 339
図110 メール暗号化(E-mail Encryption):Eメール暗号化の有効化 340
図111 メール暗号化(E-mail Encryption):オプション 341
図112 メール暗号化(E-mail Encryption):内部ユーザのリスト 342
図113 メール暗号化(E-mail Encryption):S/MIME認証局のリスト 345
図114 メール暗号化(E-mail Encryption):S/MIME証明書のリスト 347
図115 メール暗号化(E-mail Encryption):OpenPGP公開鍵のリスト 348
図116 当製品の隔離レポート Astaro Security Gateway 349
図117 隔離レポート:隔離レポートの有効化 351
図118 隔離レポート:除外 352
図119 隔離レポート:詳細オプション 354
図120 メールマネージャ - Astaro Security Gateway 356
図121 メールマネージャ:概要 361
図122 メールマネージャ:設定 363
図123 ワイヤレスセキュリティ(Wireless Security):グローバル設定 366
図124 ワイヤレスセキュリティ(Wireless Security):ワイヤレスネットワーク 369
図125 ワイヤレスセキュリティ:アクセスポイント 372
図126 ワイヤレスセキュリティ:アクセスポイントおよびSSIDグルーピング 374
図127 ワイヤレスセキュリティ(Wireless Security):クライアント 375
図128 RED:セットアップの略図 389
図129 RED:概要ページのサイトのステータス 390
図130 サイト間VPN IPsec:接続リスト 413
図131 サイト間VPN IPsec:リモートゲートウェイリスト 414
図132 サイト間VPN IPsec:ポリシリスト 418
図133 サイト間VPN IPsec:ローカルRSA鍵の設定 422
図134 サイト間VPN IPsec:詳細設定 424
図135 サイト間SSL VPN:サーバ接続の設定 427
図136 サイト間SSL VPN:クライアント接続の設定 429
図137 サイト間SSL VPN:設定 431
図138 サイト間SSL VPN:詳細設定 433
図139 証明書管理:証明書のリスト 435

図140 証明書管理:認証局リスト........ 438
図141 証明書管理:失効リスト(CRL)の一覧........ 439
図142 証明書管理:詳細設定........ 440
図143 ユーザポータル:リモートアクセスインストールファイル........ 441
図144 リモートアクセスSSL:SSLリモートアクセスの有効化........ 443
図145 リモートアクセスSSL:設定........ 444
図146 リモートアクセスSSL:詳細設定........ 446
図147 PPTPリモートアクセス:PPTPリモートアクセスの有効化........ 448
図148 PPTPリモートアクセス:iOSデバイス設定........ 450
図149 PPTPリモートアクセス:詳細設定........ 451
図150 リモートアクセスL2TP:L2TPリモートアクセスを有効にする........ 452
図151 リモートアクセスL2TP:iOSデバイス設定........ 455
図152 リモートアクセスL2TP:詳細設定........ 456
図153 リモートアクセスIPsec:接続リスト........ 459
図154 リモートアクセスIPsec:ポリシリスト........ 462
図155 リモートアクセスIPsec:詳細設定........ 466
図156 Cisco VPNクライアント:Cisco VPNクライアント経由のリモートアクセスの有効化........ 469
図157 Cisco VPNクライアント:iOSデバイス設定........ 471
図158 リモートアクセス(Remote Access):詳細設定........ 473
図159 レポーティング:Flashベースの折れ線グラフの例........ 476
図160 レポーティング:Flashベースの円グラフの例........ 477
図161 ログ:今日のログファイル........ 477
図162 ログ:アーカイブログファイル........ 478
図163 ログ:ログファイルの検索........ 479
図164 レポーティング(Reporting):CPU使用状況のヒストグラム........ 480
図165 レポーティング(Reporting):メモリ/スワップ使用状況のヒストグラム........ 481
図166 レポーティング(Reporting):パーティション使用状況のヒストグラム........ 481
図167 レポーティング:イーサネットインタフェース使用状況のヒストグラム........ 483
図168 レポーティング:上位サービス順にソートされた帯域幅使用状況データ........ 485
図169 レポーティング:ファイアウォール違反のヒストグラム(デイリー)........ 487
図170 レポーティング:侵入防御イベントのヒストグラム(マンスリー)........ 487
図171 レポーティング:シングルユーザの非匿名化........ 498
図172 レポーティング:メールフローのヒストグラム........ 500
図173 レポーティング:最もアクティブなEメールアドレスのランキング........ 500
図174 レポーティング:Eメールアドレスとドメインの非匿名化........ 501
図175 レポーティング:最後の30日間の完了したセッション接続........ 503

図 176 レポーティング: Webアプリケーションファイアウォールのマイスリーアクティビティのヒストグラム 504
図 177 レポーティング(Reporting) : デイリーエグゼクティブレポートの設定 506
図 178 ログ: ローカルログの有効化 507
図 179 ログ: リモートSyslogサーバの設定 509
図 180 ログ: リモートログファイルアーカイブの設定 511
図 181 レポーティング: ユーザデータの匿名化の有効化 515
図 182 サポート(Support) : ダウンロード - 管理ガイド / Astaro Security Gateway 518
図 183 サポート(Support) : pingを使用したホストの可用性チェック 520
図 184 サポート(Support) : tracerouteを使用したルートの確認 521
図 185 サポート(Support) : digを使用したDNSエントリのルックアップ 522